ЗАЩИТА ОБОРУДОВАНИЯ ПОДСТАНЦИЙ

от электромагнитного импульса

Владимир Гуревич

«Инфра-Инженерия»

В.И. Гуревич

ЗАЩИТА ОБОРУДОВАНИЯ ПОДСТАНЦИЙ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

Учебно-практическое пособие

Москва
Инфра-Инженерия
2016

УДК 621.316.925(075.8)
ББК 31.27-05
Г 95

Гуревич В.И.
Г 95 Защита оборудования подстанций от электромагнитного импульса. – М.: Инфра-Инженерия, 2016. – 302 с.: ил.

ISBN 978-5-9729-0104-3

В книге рассмотрены практические аспекты защиты электрооборудования подстанций на примере микропроцессорных устройств релейной защиты (МУРЗ) и силовых трансформаторов от разрушительного воздействия электромагнитного импульса высотного ядерного взрыва и других видов преднамеренных электромагнитных деструктивных воздействий, оборудование для производства которых интенсивно разрабатывают и совершенствуют в последние годы.

Предложены различные технические решения и организационные мероприятия, направленные на повышение живучести подстанций.

Книга рассчитана на специалистов, занимающихся эксплуатацией электрооборудования на подстанциях, проектировщиков, производителей МУРЗ, руководителей отрасли, а также может быть полезна преподавателям, аспирантам и студентам вузов, специализирующихся в области электроэнергетики.

ISBN 978-5-9729-0104-3

АВТОР

Владимир Игоревич Гуревич – родился в г. Харькове (Украина) в 1956 г. В 1978 г. окончил факультет электрификации Харьковского национального технического университета им. П.Василенко по специальности «Электроснабжение с.х.». С 1980 по 1983 г. учился в аспирантуре. В 1986 г. защитил кандидатскую диссертацию в Национальном техническом университете «Харьковский политехнический институт» по специальности «Электрические аппараты».

Работал преподавателем, и.о. доцента Харьковского национального технического университета им. П. Василенко, главным инженером и директором Научно-технического предприятия «Инвентор» (г. Харьков). Руководил несколькими проектами по разработке новых видов аппаратуры, выполняемых по заказам Министерств оборонных отраслей промышленности СССР, после распада СССР занимался разработкой и организацией производства устройств автоматики для электроэнергетики. В настоящее время работает в Электрической компании Израиля в должности ведущего инженера-специалиста, начальника сектора Центральной электрической лаборатории.

С 2006 г. Почетный профессор Харьковского национального технического университета им. П. Василенко. С 2007 г. эксперт комитета ТС-94 Международной электротехнической комиссии (МЭК).

В.И. Гуревич автор 13 книг (6 из которых изданы в США), свыше 120 изобретений и свыше 190 научно-технических статей.

В издательстве «Инфра-Инженерия» вышли следующие книги автора:

- Микропроцессорные реле защиты. Устройство, проблемы, перспективы, 2011, 336 с.

- Устройства электропитания релейной защиты: проблемы и решения, 2013, 228 с.

- Уязвимости микропроцессорных реле защиты: проблемы и решения, 2014, 256 с.

ООО НПП «ЭКРА» – научно-производственное предприятие «полного цикла», созданное в 1991 году российскими специалистами-релейщиками в г. Чебоксары и функционирующее без участия иностранного капитала. Предприятие специализируется на выпуске наукоемких комплектных устройств релейной защиты, автоматики и управления на новейшей микропроцессорной элементной базе, адаптированных к применению в составе систем АСУ ТП.

Деятельность ООО НПП «ЭКРА» включает в себя:

- *научно-исследовательские и опытно-конструкторские разработки;*
- *проектные работы;*
- *производство;*
- *заводские испытания;*
- *шеф-наладку на объекте;*
- *обучение;*
- *гарантийное и сервисное обслуживание.*

Предприятие выпускает на собственной производственной базе:

- *микропроцессорные комплектные устройства защиты генераторов, трансформаторов и блоков генератор-трансформатор любых мощностей для электростанций;*
- *микропроцессорные комплектные устройства релейной защиты и автоматики (РЗА) подстанционного оборудования 6-750 кВ;*
- *противоаварийная автоматика;*
- *цифровые аварийные осциллографы;*
- *программно-технический комплекс (ПТК) для АСУ ТП подстанций;*
- *системы оперативного постоянного тока;*
- *щиты собственных нужд;*
- *низковольтные комплектные устройства (НКУ);*
- *устройства плавного пуска и регулирования скорости двигателей напряжением 3-15 кВ мощностью до 17 МВт;*
- *преобразователи частоты для двигателей 3-10 кВ;*
- *статический возбудитель для синхронных двигателей мощностью до 12,5 МВт;*
- *оборудование ВЧ связи.*

Система менеджмента качества НПП «ЭКРА» сертифицирована на соответствие международному стандарту ISO 9001:2008. Выпускаемые предприятием устройства аттестованы для применения на энергообъектах ОАО «ФСК ЕЭС», ОАО «РусГидро», ОАО «Концерн «Росэнергоатом», ОАО «Газпром», АК «Транснефть».

НПП «ЭКРА» аккредитовано Федеральной Службой по экологическому, технологическому и атомному надзору на право конструирования и изготовления оборудования для объектов атомной энергетики по 4-му и 3-му классу

безопасности. Более 500 шкафов микропроцессорных устройств РЗА, а также низковольтных комплектных устройств установлены на 10-ти атомных станциях нашей страны. Спектр выпускаемой продукции и предоставляемых предприятием услуг для объектов атомной энергетики постоянно расширяется.

Особенности применения оборудования НПП «ЭКРА»:

1. Все имеющиеся решения на базе устройств НПП «ЭКРА» в части РЗА и ПА электрических станций и подстанций классов напряжения от 6 до 750кВ позволяют заменить практически 100% соответствующих устройств зарубежных производителей.

2. Применяемые НПП «ЭКРА» решения в части РЗА полностью отвечают отечественной идеологии построения комплекса РЗА электрических станций и подстанций, что позволяет обслуживающему персоналу подстанции легко адаптироваться при переходе с устаревших панелей защит на современные микропроцессорные. При использовании устройств РЗА зарубежных производителей необходимо провести большую работу по адаптации имеющегося технического решения под отечественные нужды, что приводит к увеличению сроков, стоимости и конечной надежности комплекса РЗА (в случае ошибок при конфигурации устройств).

3. Выпускаемая на НПП «ЭКРА» продукция по своему функционалу и надежности не уступает продукции ведущих мировых производителей релейной защиты и автоматики, однако имеет более низкую стоимость по сравнению с аналогичным оборудованием зарубежных производителей.

4. Все серийно производимые устройства РЗА 6-750кВ соответствуют требованиям стандарта МЭК61850. Устройствами поддерживаются протоколы связи согласно части стандарта МЭК 61850-8-1.

5. Для подстанций нового поколения, так называемых «Цифровых подстанций», имеются специализированные исполнения терминалов с поддержкой стандарта МЭК61850-9-2LE. Данные решения внедрены и проходят опытную эксплуатацию на ПС 220кВ «Чистополь» (Республика Татарстан, ОАО «Сетевая компания), ПС 220кВ «Венец» (Чувашская Республика, ОАО «ФСК ЕЭС»), Нижегородской ГЭС (ОАО «РусГидро»).

6. Обновление программного обеспечения производится более оперативно, чем у зарубежных производителей. При этом новое программное обеспечение изначально написано для русскоязычных пользователей, что минимизирует ошибки при пользовании программным продуктом.

7. Специалистами НПП «ЭКРА» осуществляется круглосуточная техническая поддержка. В случае применения импортного оборудования вопросы с заводом-изготовителем зачастую приходится решать на иностранном языке.

8. Имеется широкая сеть сервисных центров на всей территории России. Ремонт оборудования осуществляется в срок до 24 часов. При использовании оборудования зарубежных производителей сроки обслуживания и ремонта значительно увеличиваются.

Предприятие вкладывает значительные средства в расширение и обновление производства. Производственные площади составляют более 25 000 кв. метров, включая собственное производство металлоконструкций с оборудованием по металлообработке, гибке и лазерной резке, гальваническому и порошковому покрытиям. Имеющийся производственный потенциал позволяет выпускать около 4 тысяч шкафов в год. В связи с ежегодно возрастающими объёмами выпускаемой продукции, в 2011 году началось строительство нового производственного комплекса. В июне 2014 года состоялся торжественный пуск первой очереди многофункционального производственного комплекса, рассчитанного на выпуск 2000 шкафов НКУ и 200 единиц преобразователей частоты в год. Весь производственный комплекс позволит выпускать до 7000 шкафов релейной защиты, 4000 шкафов НКУ и 300 преобразователей. Запуск второй и третьей очередей планируется в 2015 и 2016 годах, соответственно.

Открыты региональные представительства: ООО «ЭКРА-Центр» (г. Москва), ООО «ЭКРА-Сибирь» (г. Красноярск), ООО «ЭКРА-Восток» (г. Хабаровск), ООО «ЭКРА-Юг» (г. Пятигорск), ООО «ЭКРА-Северо-Запад» (г. Санкт-Петербург), ООО «ЭКРА-Урал» (г. Екатеринбург), ТОО «ЭКРА Казахстан» (г. Алматы), «EKRA-ASIA» (г. Ташкент), «ЭКРА-Туркмен» (г. Ашхабад).

Продукцией НПП «ЭКРА» оснащено более 320 электростанций, 1800 подстанций классов напряжений 35-110-220 кВ, 177 подстанций класса напряжения 330-750 кВ и энергообъектов других отраслей промышленности. Оборудование НПП «ЭКРА» установлено в России и 10-ти зарубежных странах: Афганистан, Бангладеш, Вьетнам, Грузия, Ирак, Казахстан, Кыргызстан, Таджикистан, Узбекистан, Украина.

НПП «ЭКРА» готово предоставить потребителям широкий спектр оборудования собственного производства, отвечающего всем современным требованиям.

Адрес: Россия, 428003, Чувашская Республика,
г. Чебоксары, пр. И. Яковлева, д. 3
Телефон/факс: (8352) 22-01-10, 22-01-30 (автосекретарь)
web: http://www.ekra.ru
e-mail: ekra@ekra.ru

ПРЕДИСЛОВИЕ

Еще каких-нибудь 20 лет тому назад упоминание об электромагнитном импульсе ядерного взрыва (ЭМИ ЯВ) можно было встретить в русскоязычной литературе лишь в брошюрках по гражданской обороне. Причем, именно краткое упоминание и не более того. Поэтому и воспринимается этот импульс как нечто весьма экзотическое и малопонятное. Военные, конечно, были хорошо осведомлены об этом эффекте ЯВ, но все сведения на эту тему тщательно засекречивали. В то время это было вполне оправдано, учитывая с какими техническими сложностями и материальными затратами эти сведения добывались. Однако в результате такой политики гражданские специалисты в различных отраслях техники до недавнего времени понятия не имели (а некоторые и до сих пор не имеют) об этом явлении и опасности, которую оно представляет.

Между тем, современные тенденции развития техники, заключающиеся в расширяющемся повсеместном применении микроэлектроники, микропроцессоров, компьютеров, быстром росте производительности микропроцессоров, сопровождающемся резким увеличением количества микротранзисторов, приходящихся на единицу объема, снижением рабочих напряжений и уровней изоляции между внутренними элементами и слоями в кристалле, привели к резкому возрастанию уязвимости современной техники к ЭМИ ЯВ, с одной стороны, и к стимулированию интереса военных к использованию ЭМИ ЯВ в качестве самостоятельного и очень эффективного вида оружия – с другой. Если ранее этот поражающий фактор ЯВ интересовал военных лишь с точки зрения надежного поражения электронных систем самолетов и ракет противника силами противовоздушной обороны (боевые части многих ракет различных систем ПВО, даже небольшой дальности снабжались ядерными зарядами), то теперь пришло понимание того, что ЭМИ ЯВ является идеальным нелетальным оружием, позволяющем при подрыве ядерного заряда на большой высоте вывести из строя практически всю инфраструктуру противника без массового убийства людей. Это настолько воодушевило военных, что они заказали разработку специального ядерного заряда с усиленным эффектом электромагнитного импульса – так называемого «супер-ЭМИ». Параллельно, ускоренными темпами началась разработка чисто электромагнитного оружия, в котором мощное электромагнитное излучение, поражающее современные микроэлектронные и микропроцессорные системы, формируется неядерными средствами. Электромагнитные бомбы, снаряды, гранаты, ракеты с электромагнитными боеголовками, передвижные установки на колесном и гусеничном ходу, обеспечивающие мощное направленное излучение, поражающее электронику на большом расстоянии – все это уже давно не фантастика, а реалии нашего времени. С сожалением можно констатировать, что эти реалии по-прежнему остаются без достаточного внимания

специалистов во многих областях техники, в частности, в области электроэнергетики. А ведь электроэнергетика – это основа инфраструктуры страны, без которой не возможно функционирование ни водоснабжения, ни связи, ни других важнейших систем жизнеобеспечения.

В ряде предыдущих статей и книг автора обращалось внимание специалистов на актуальность этой проблемы в связи с возрастанием опасности разрушения электроэнергетической системы такими видами оружия. В данной книге сделан упор на практические рекомендации по защите электрооборудования подстанций от преднамеренных электромагнитных деструктивных воздействий, включая ЭМИ ЯВ.

Следует особо отметить, что защита электрооборудования подстанций (да и других объектов электроэнергетики) от таких воздействий – проблема не только самих энергетиков, но и промышленности, производящей микроэлектронную и микропроцессорную аппаратуру для энергетики. Поэтому рекомендации, приведенные в книге, предназначены не только для персонала, занимающегося эксплуатацией электрооборудования, но также и для производителей такого оборудования, в первую очередь микропроцессорных устройств релейной защиты, специалистов проектных организаций, руководителей электроэнергетической отрасли, а также преподавателей, аспирантов и студентов электроэнергетических специальностей вузов.

Только совместными усилиями специалистов можно предотвратить надвигающуюся опасность.

Отзывы на книгу просьба направлять автору по адресу: vladimir.gurevich@gmail.com

Автор

1. ТЕХНИЧЕСКИЙ ПРОГРЕСС И ЕГО ПОСЛЕДСТВИЯ

1.1. Философия технического прогресса

Рационально планируемое развитие техники все чаще приводит к иррациональным последствиям, и техника выступает в сознании человека не как нейтральное средство для удовлетворения его потребностей, а как самостоятельная цель, отчужденная сила.

/докт. фил. наук, проф. Попкова Н. В./

Что такое технический прогресс? Философская энциклопедия дает такое определение:

> *«Технический прогресс — взаимообусловленное, взаимостимулирующее развитие науки и техники. Понятие было введено в 20 в. в контексте обоснования, использующего потребительное отношение к природе, и традиционной научно-инженерной картины мира. Цель технического прогресса определяется как удовлетворение постоянно растущих потребностей человека; способ удовлетворения этих потребностей — реализация достижений естественных наук и техники».*

Действительно, как пишет докт. фил. наук, проф. Попкова Н.В. в своей статье «Философия техники» [1], технологические инновации вводились людьми для улучшения жизни и удовлетворения потребностей: эту задачу техногенная среда выполняет, давая возможность все увеличивающемуся населению Земли получать материальные предпосылки существования. Но в последние годы все полнее проявляются другие последствия технологического роста: подавление собственно биологических и гуманитарных сторон жизни человека, вытеснение их техногенными качествами и закономерностями. Это вызывает двойственную оценку роли техногенной среды: ранее преобладавшую позитивную и набирающую вес негативную. Основная проблема заключается в трудностях управления техногенной средой, в невозможности контролировать ее развитие или хотя бы прогнозировать ее реакцию на внедрение оче-

редных инноваций. Выявление на всех этапах технической деятельности непредсказуемых и нежелательных ее результатов показывает: *техногенная среда всегда находилась отчасти вне контроля создающего ее человечества, а значит, обладала автономностью*.

Таким образом, далеко не всегда развитие техники направлено на «*удовлетворение постоянно растущих потребностей человека»,* причем по нашим наблюдениям, такое свойство технический прогресс начал приобретать лишь во второй половине 20-го века.

В одном старом научно-фантастическом романе был представлен занятный сюжет, развитие которого началось с довольно невинной вещи: необычного ночного звонка на все телефоны всем жителям планеты Земля. Этим звонком всем людям Земли возвестил о своем рождении Глобальный Разум. Оказалось, что на каком-то этапе развития количественный рост компьютеров перерос в новое качество: миллионы компьютеров, объединенных в общую сеть и управляющих всем и вся на планете Земля, вдруг осознали себя как единое целое, способное к самовоспроизводству посредством автоматизированных заводов и роботов, включенных в ту же сеть, а также к защите с помощью компьютеризированных систем вооружения, рассчитанных на уничтожение человека. С точки зрения Глобального Разума человечество было ничем иным, как рудиментом, балластом, пожирающим ресурсы планеты. Дальнейшее развитие сюжета читатели могут предугадать сами.

Компьютерами с сетевым подключением уже сегодня управляются практически все виды современных промышленных производств, системы управления водоснабжением и электроснабжением, системы телекоммуникации и связи. В технической, а не в фантастической литературе появились термины: «разумная электрическая сеть» (Smart Grid), релейная защита с «искусственным интеллектом» (Artificial Intelligence). В технической, а не в фантастической литературе рассматриваются сегодня вопросы создания «умного жилища» (Smart House), в котором даже холодильник будет сам оценивать запасы хранящихся в нем продуктов, и на основе анализа их потребления будет составлять заказ и отсылать его по сети в ближайший супермаркет. Сегодня микропроцессоры можно найти уже где угодно, даже в крышке унитаза.

Человечество семимильными шагами движется к созданию непредсказуемого Глобального Разума, предугаданного в старом фан-

тастическом романе. Поэтому этот старый сюжет уже давно перекочевал со страниц фантастических романов на страницы серьезных философских журналов и книг, освещающих проблемы философии техники. Это относительно новая область философских исследований, направленных на осмысление природы техники и оценку ее воздействий на общество, культуру и человека. Существует точка зрения, согласно которой философия техники – это скорее не собственно философия, а междисциплинарная область знаний, для которой характерно самое широкое рассмотрение техники и осмысление проблем создаваемых ею.

На симпозиуме VISION-21, который проводился в 1993 году Центром космических исследований NASA им. Льюиса и Аэрокосмическим институтом Огайо, прозвучало нашумевшее выступление известного математика профессора Вернора Винджа [2]:

> "*Ускорение технического прогресса - основная особенность XX века. Мы на грани перемен, сравнимых с появлением на Земле человека. Сугубая причина этих перемен заключается в том, что развитие техники неизбежно ведёт к созданию сущностей с интеллектом, превышающим человеческий.... Крупные компьютерные сети (и их объединенные пользователи) могут "осознать себя" как сверхчеловечески разумные сущности... Такое событие аннулирует за ненадобностью весь свод человеческих законов, возможно, в мгновение ока. Неуправляемая цепная реакция начнет развиваться по экспоненте безо всякой надежды на восстановление контроля над ситуацией*".

Виндж предложил новый термин для этого явления: "***Технологическая сингулярность***". Обычно, под сингулярностью понимается некая особая точка или область функции, значение в которой стремится к бесконечности или имеет какие-либо иные нерегулярности поведения, это некая критическая точка, после которой значение функции становится неопределенным и непредсказуемым. Типичные примеры сингулярности – лавинный пробой в полупроводниковых структурах, туннельный эффект в электрических контактах и в полупроводниках, участок вольтамперной характеристики туннельного диода и т.д. Технологическая сингулярность подразумевает некую точку в развитии техники вообще, а компьютерной

техники и искусственного интеллекта особенно, после которой дальнейшее их развитие становится, во-первых, необратимо и не зависимо от человека, а во-вторых, непредсказуемо.

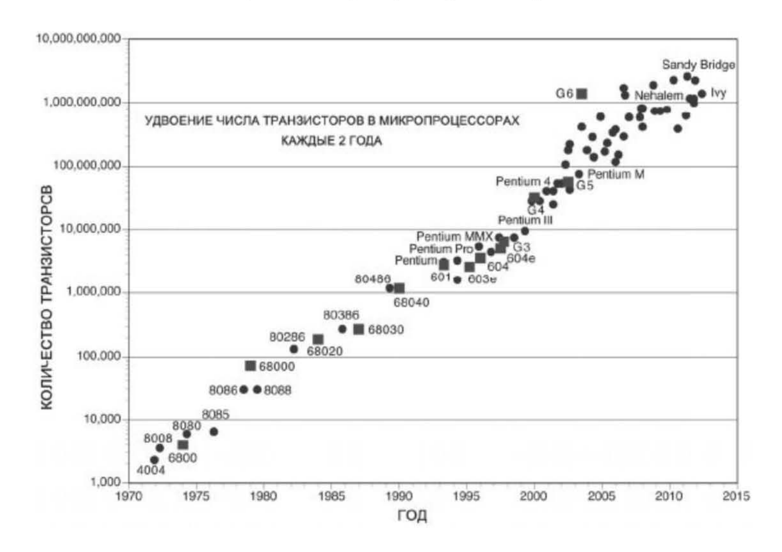


Рис. 1. 1. Зависимость числа транзисторов на кристалле микропроцессора от времени. Вертикальная ось имеет логарифмическую шкалу, поэтому зависимость соответствует экспоненциальному закону

На взгляды Винджа повлиял, безусловно, так называемый Закон Мура (Мора) [3], сформулированный в 1965 году одним из учредителей компании Intel Гордоном Муром (Gordon Moor). Этот закон гласит, что количество транзисторов в микропроцессорах удваивается примерно каждые 2 года, а их производительность растет экспоненциально, рис. 1.1. Этот закон действует более 50 лет. По такому же экспоненциальному закону развивается, постоянно усложняясь, не только микропроцессорная и компьютерная техника, но и другие виды техники, а за ними и общество. Социолог М. Сухарев в своей работе «Взрыв сложности» [4] пишет:

«В развитии общества видна еще одна закономерность - ускорение роста сложности со временем. Десятки тысяч лет жили на Земле племена, вооруженные копьями и луками. За несколько сотен лет мы проскочили промышленно-техническую цивилизацию. Сколько лет отпущено компьютерному этапу, не известно, но нынешняя скорость эволюции общества беспрецедентна».

Подтверждают эту мысль многие крупнейшие специалисты:
- доктор философских наук профессор И. А. Негодаев [5]: *«Закономерностью развития техники является ее последовательное усложнение. Это усложнение происходит как путем увеличения числа элементов входящих в техническую систему, так и изменением ее структуры»;*
- директор, главный конструктор Центрального научно-исследовательского и опытно-конструкторского института робототехники и технической кибернетики, член-корреспондент РАН В. А. Лопота и докт. техн. наук, проф. Е. И. Юревич [6]: «*Общая закономерность научно-технического развития во всех сферах человеческой деятельности - прогрессирующее усложнение, интеграция и интенсификация техники»;*
- канд. техн. наук Безменов А. Е. [7]: «*Тенденция развития техники характеризуется все* большим усложнением машин, *приборов и установок. С увеличением сложности изделий их надежность (при прочих равных условиях) уменьшается»*.

Если «взрыв сложности» бытовой техники происходит у всех нас на виду и не требует доказательств, то усложнение техники в промышленности не так заметно для обывателя. Поэтому рассмотрим несколько конкретных примеров, подтверждающих эту тенденцию.

Всемирно известная шведская компания Programma Electric AB, созданная в 1976 г. (которая в 2001 г. была приобретена General Electric, а в 2007 г. вошла в состав концерна Megger Group Ltd) выпускает огромную номенклатуру приборов и устройств для тестирования электроэнергетического оборудования: от точных таймеров и систем для проверки реле защиты, до источников сильных токов. Одним из изделий этой компании является устройство типа B10E,

рис. 1.2, для измерения минимального напряжения срабатывания приводов высоковольтных выключателей.

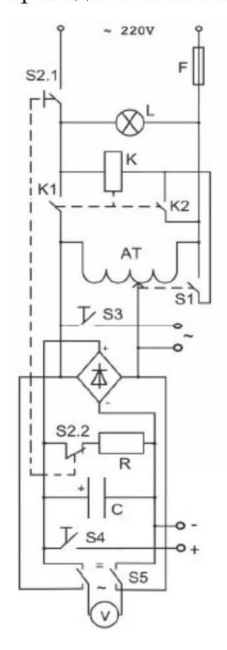


Рис. 1.2. Внешний вид устройства типа B10E для проверки минимального напряжения срабатывания приводов высоковольтных выключателей

Рис. 1.3. Пример схемы простого устройства для проверки высоковольтных выключателей, реализующей все необходимые функции

В соответствии со стандартом МЭК 62271-100 такие выключатели подлежат проверке на соответствие параметрам производителя по минимальному напряжению срабатывания. В общем-то, речь идет о прибое, выполняющем очень простую функцию: предварительную установку определенного уровня напряжения, контролируемого вольтметром, с последующей подачей этого напряжения на выходные клеммы прибора. Разработать схему устройства, реализующего эту функцию не сложно, рис. 1.3. В этом устройстве выходное напряжение устанавливается лабораторным автотрансформатором AT типа ЛАТР-9, выпрямляется диодным мостом и сглаживается конденсатором C большой емкости (несколько тысяч микрофарад). На одну пару выходных клемм подается регулируемое переменное напряжение, на другую – регулируемое постоянное напряжение. Контроль выходных напряжений осуществляется с помощью вольтметра V. Для предотвращения случайной подачи

высокого напряжения (250 В) с устройства на низковольтную (24-48 В) катушку или на мотор, на автотрансформаторе установлен микропереключатель S1 таким образом, что его контакты замкнуты под действием толкателя, укрепленного на валу, только в нулевом положении движка автотрансформатора. При нажатии кнопки S2 происходит отключение разрядного резистора R от конденсатора C и подача напряжения на вход устройства. Для подачи на катушки выключателя предварительно выставленного с помощью вольтметра и автотрансформатора напряжения, в дополнение к удерживаемой кнопке S2 нажимают одну из кнопок S3 (выход переменного тока) или S4 (выход постоянного тока). Если выключатель не сработал, увеличивают напряжение, удерживая кнопку S2, и опять нажимают одну из кнопок S3 или S4.

А теперь посмотрим, как этот простейший алгоритм реализован в устройстве B10E известной фирмы, рис. 1.4а.

Рис. 1.4а. Электронный блок устройства B10E. Полупроводниковые приборы, установленные по краям печатной платы, прижимаются при сборке к радиатору, которым служит корпус устройства

Электронный блок устройства, рис. 1.4а, содержит 13 электромагнитных реле, 14 микросхем различного назначения, 10 выпрямительных диодных мостов на ток 1А и два мощных диода типа 40EPS08 (40А, 800В); 4 мощных транзистора типа BUX98AP (24А, 1000В); 3 мощных симистора типа BTA26-400B (25А, 400В); 4

мощных запираемых тиристора – GTO (13.5А, 800В); 2 прецизионных токовых шунта типа PBV, ну и так далее. Признаюсь честно, когда я открыл это устройство с целью его ремонта, то был просто в шоке от увиденного. Особенно меня умилил электронный датчик угла поворота вала автотрансформатора вместо простейшего микропереключателя (как на рис. 3).

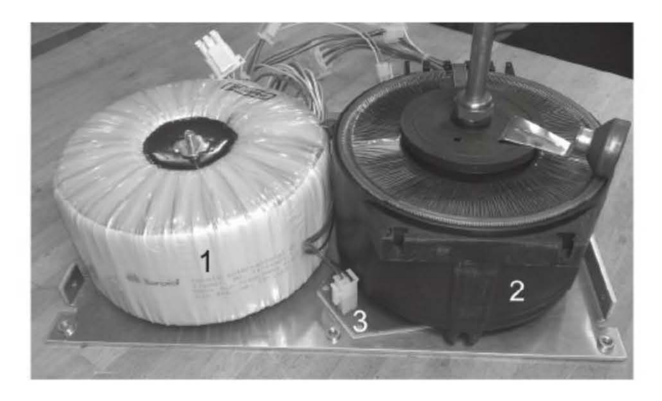


Рис. 1.4б. Силовой блок устройства B10E: 1 – многообмоточный трансформатор с набором различных выходных напряжений для питания электронных узлов устройства; 2 – регулируемый автотрансформатор; 3 – плата датчика угла поворота вала автотрансформатора

Налицо полное несоответствие простейших функций, выполняемых устройством, с его технической реализацией. Интересно, какое оправдание всему этому нагромождению электроники дали бы разработчики этого устройства?

А вот еще один пример из области выпрямительных зарядно-подзарядных агрегатов (ВЗПА), широко применяемых на электростанциях и подстанциях в системах оперативного постоянного тока. Такой агрегат состоит из следующих основных узлов: силового трансформатора, блока силовых тиристоров и электронного блока управления тиристорами. В начале 70-х годов прошлого века фирмой AEG был разработан электронный блок управления тиристорами ВЗПА, рис. 1.5, который оказался настолько удачным, что применяется вот уже более сорока лет различными производителями в

различных моделях ВАЗП. Причем, некоторые производители просто полностью скопировали этот блок управления, а некоторые перевели его на современную элементную базу, рис. 1.6, что, конечно, не меняет сути.

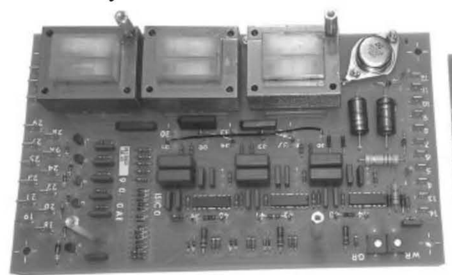
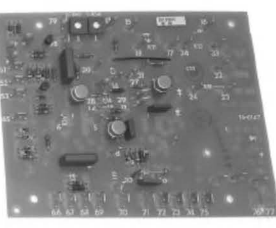



Рис. 1.5. Два модуля блока управления тиристорами ВЗПА, разработанные и выпускавшиеся в массовом количестве с 70-х годов прошлого столетия компанией AEG. Справа – аналоговый модуль, контролирующий выходной ток ВЗПА и выдающий сигнал на импульсный модуль (слева), формирующий импульсы управления тиристорами

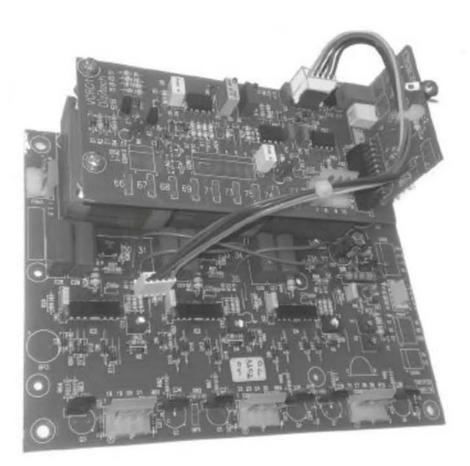


Рис. 1.6. Блок управления тиристорами ВЗПА, выполненный на современной элементной базе по схеме, разработанной AEG в 70-х годах прошлого века

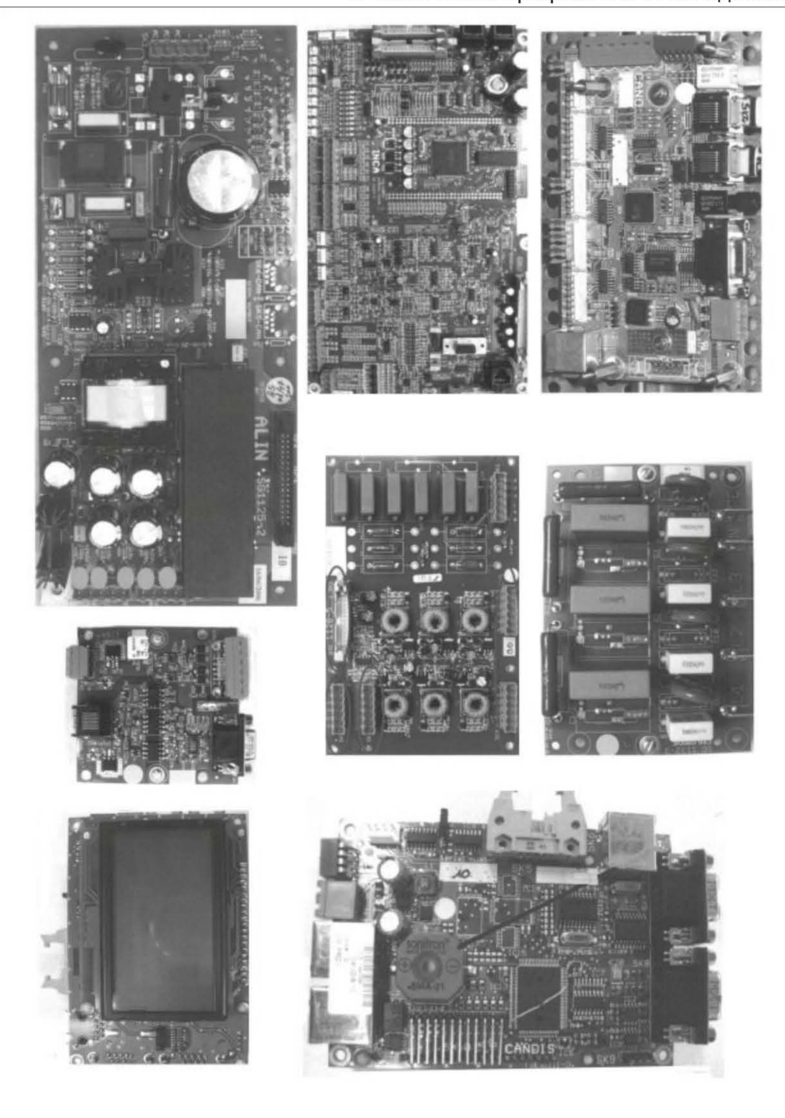


Рис. 1.7а. Комплект основных модулей микропроцессорного ВЗПА серии Apodys фирмы Chloride France S.A.

Рис. 1.7б. ВЗПА серии Apodys фирмы Chloride France S.A., входящей в концерн Emerson

К сожалению, как ни хорошо зарекомендовала себя аналоговая техника в системе управления ВЗПА на протяжении почти 45 лет, и по надежности и по ремонтопригодности, к настоящему времени можно констатировать, что она уже почти полностью вытеснена цифровыми устройствами на базе микропроцессоров. Какие же новые качества приобрели современные ВЗПА с микропроцессорным управлением, рис. 1.7б.

Да вот какие: «ветвистое» меню в котором не так-то просто разыскать нужную функцию вместо трех потенциометров регулирования выходного напряжения и переключателя режимов работы; IP-адрес и сетевое подключение, позволяющее вмешиваться в работу ВЗПА хакерам; модемная связь между внутренними модулями вместо обычных медных проводов и так далее.

Рис. 1.8. Устройство типа МСТ1600 фирмы Megger для проверки трансформаторов тока

Описание примеров «взрыва сложности» можно было бы продолжать. Например, можно было бы упомянуть устройство типа MCT1600 фирмы Megger, рис. 1.8, для проверки сопротивления изоляции, коэффициента трансформации и точки перегиба вольт-амперной характеристики трансформаторов тока, которое при включении загружает полноценную операционную систему VX Works (64–битная операционная система реального времени).

Или измерители сопротивления той же фирмы, прошедшие эволюцию от миниатюрного приборчика с генератором, вращаемым ручкой, до чрезвычайно сложных микропроцессорных агрегатов, рис. 1.9.

Типичный пример «взрыва сложности» в электроэнергетике – это Smart Grid. Известно, что концепция «умной сети» предполагает установку микропроцессоров на все без исключения элементы системы производства, распределения и учета электроэнергии и организацию между ними информационных каналов на основе компьютерных сетей, преимущественно беспроводных (Wi-Fi). По идее апологетов Smart Grid энергосистема будущего должна выглядеть как современная навороченная сетевая компьютерная игра с тысячами участников – компонентов электрических сетей. Одним из центральных участников этой «игры» является микропроцессорная релейная защита: с искусственным интеллектом, самоадаптируемая, с недетерминированной логикой, упреждающего действия, то есть действующая самостоятельно и по своему усмотрению [8].

Рис. 1.9. Приборы для измерения сопротивления изоляции производства фирмы Megger: WM6 – простейший прибор с генератором и рукояткой для вращения якоря; S1-5010 – сложнейшее микропроцессорное устройство

Дешевизна и доступность микропроцессоров, промышленных контроллеров и современных электронных компонентов высокой степени интеграции, огромная и все расширяющаяся номенклатура таких компонентов, имеющихся на рынке, чрезвычайно высокая производительность оборудования, предназначенного для автоматической установки и распайки элементов поверхностного монтажа на печатную плату, автоматические системы тестирования готовых печатных плат – все это снимает имевшиеся ранее ограничения на сложность электронных систем и область их применения. В связи с чем, микропроцессоры сегодня можно найти уже повсюду. Такое быстро расширяющееся применение электронных узлов на основе микропроцессоров во всех областях техники при непрекращающемся их усложнении и является сегодня определяющей тенденцией развития техники. Апологеты технического прогресса в его нынешнем виде пытаются убедить всех в том, что такое непрерывное и все нарастающее усложнение техники и есть «технический прогресс». Конечно, есть такие области техники и технологии, в которых без вычислительных операций и без микропроцессоров просто не обойтись и микропроцессорная техника действительно позволила совершить технологический скачек. Однако далеко не во всех случаях применения микропроцессорной техники реально обосновано техническими требованиями к изделию, причем количество таких случаев растет как снежный ком и приведенные выше примеры лишь слабая иллюстрация этого процесса.

Но если усложнение техники часто совершенно не оправдано, как было показано выше, то почему же она все-таки непрерывно усложняется, причем, все возрастающими темпами? Ответ достаточно прост: в постоянном усложнении техники заинтересованы разработчики и производители, так как такое постоянное и целенаправленное усложнение позволяет им достичь сразу несколько целей:

- во-первых, повысить эффективности рекламной кампании, предлагая потребителю все большее количество новых функций в новых изделиях (далеко не всегда действительно нужных);

- во-вторых, снижать надежность и срок службы (что является естественным результатом усложнения), то есть заставлять потребителя чаще приобретать новую продукцию;

- в-третьих, постоянно снижать ремонтопригодность производимой продукции и усиливать зависимость покупателя от производителя. Самые современные электронные устройства и приборы, выполненные по технологии поверхностного монтажа, допускают ремонт только путем замены целых блоков, производимых все тем же производителем. Во многих случаях, стоимость этих блоков является несоразмерно высокой, но потребитель вынужден приобретать эти блоки по явно завышенной цене.

Таким образом, во многих случаях усложнение техники стало искусственным процессом, часто не имеющим объективной основы, инициируемым производителями с целью дополнительного обогащения.

Но насколько безобиден такой процесс развития техники?

По утверждению Заслуженного деятеля науки РФ, доктора технических наук, профессора, начальника 46 ЦНИИ МО РФ, генерал-майора В. М. Буренка [9]:

> “*Технологическое развитие таит в себе такое множество угроз, разнообразие и последствия, влияния которых непредсказуемы для судьбы цивилизации…. За последние годы научно-технологический прогресс подарил миру многие технические блага, а с ними и непреходящую головную боль. Примеры: компьютерные технологии и кибертерроризм, современные инфокоммуникационные системы и информационные войны, сложные системы управления инфраструктурными и техническими объектами и тяжелейшие последствия при нарушениях в их работе, познание основ жизни и генномодифицированные продукты, появление возможности искусственного выращивания опасных вирусов и т. д. Причем, многие из угроз, генерируемых новыми технологическими возможностями, проявлялись не сразу и не могли быть предсказаны (либо такого рода предсказатели числились заштатными фантастами и чудаками, которых всерьез воспринимать не стоит).*

А вот что об этом пишет академик Н. Н. Моисеев: «*...научно-технический прогресс, рост мощности цивилизации сулят не только блага. Силою, которую он дает людям, еще надо уметь пользо-*

ваться. Человек оказывается теперь в положении Гулливера, который вошел в хрустальную лавку лилипутов. Одно неосторожное движение — и все ее хрустальное великолепие превратится в гору битого стекла».

Зная о существующих опасностях, можно было бы, наверное, попытаться предотвратить их. Но вот что пишет об этом уже цитировавшийся выше известный специалист [9]:

> *«Даже когда облик какой-то технической системы уже давно сформирован, но появились новые угрозы, прогнозирование ситуации также не покажется простой задачей. Редкий аналитик возьмется, например, спрогнозировать последствия хакерской атаки на систему управления, скажем, атомной или крупной гидроэлектростанцией, систему управления воздушным или железнодорожным движением. Прогнозы типа «это будет ужасно», «неизбежны колоссальные потери» никого не устроят, а оценки типа «вероятность выброса в атмосферу радиоактивных веществ в объеме N будет равна p», «количество авиакатастроф в воздушной зоне с вероятностью p достигнет значения K» получить весьма непросто. Для того чтобы это сделать (спрогнозировать), нужны модель системы (объекта), практически адекватная реальной системе, знание уровня развития хакерского мастерства, способы проникновения в атакуемую систему и т.д. Но, во-первых, это сделать практически невозможно, а во-вторых, при наличии такой модели ее попадание в руки злоумышленников (хакеров) делает шансы на бесперебойное функционирование этой системы весьма призрачными».*

Ему вторит известный астрофизик Л. М. Гиндилис, который отмечает в своей работе [10]:

> *"Острота ситуации состоит в том, что коллапс должен наступить очень скоро, в первых десятилетиях XXI века. Поэтому, если бы даже человечество знало, как "повернуть" (или хотя бы приостановить) этот процесс, обладало бы средствами и волей для того, чтобы осуще-*

ствить поворот уже сегодня, - у него просто не хватило бы времени, так как все негативные процессы обладают определенной инерцией, в силу которой их невозможно немедленно остановить... Экономика Земли похожа на тяжело груженый транспорт, который на большой скорости мчится по бездорожью прямо к бездне. Видно, мы уже проскочили точку, где надо было свернуть, чтобы вписаться в "траекторию поворота". И затормозить тоже не успеваем. Положение усугубляется тем, что никто не знает, где находятся руль и тормоз. Тем не менее, и экипаж, и пассажиры настроены весьма благодушно, наивно полагая, что, "когда понадобится", они разберутся в устройстве транспорта и смогут совершить необходимый маневр.

В заключение приведем слова основоположника теории технологической сингулярности Вернора Винджа:

«Если технологической Сингулярности суждено быть, то она случится. Даже если все государства мира осознают "угрозу" и перепугаются до смерти, прогресс не остановится. Конкурентное преимущество - экономическое, военное, даже в сфере искусства - любого достижения в средствах автоматизации является настолько непреодолимым, что запрещение подобных технологий просто гарантирует, что кто-то другой освоит их первым. Я уже выражал сомнение в том, что мы не можем предотвратить Сингулярность, что ее наступление есть неминуемое следствие естественной человеческой соревновательности и возможностей, присущих технологиям».

Выше рассматривался естественный (если можно применить этот термин к технике) ход развития техники и технологий. Но ведь существует еще одна сторона проблемы, которая никогда не рассматривалась в философии техники. Речь идет о развивающихся параллельным курсом средствах уничтожения техники. По мере усложнения техники и все большей ее «электронизации» и «компьютеризации», растет ее уязвимость к преднамеренным дистанцион-

ным деструктивным воздействиям, включающим кибернетические и электромагнитные [11]. Поэтому разработчиками систем вооружения все большее внимание уделяется созданию новых видов оружия, направленных на поражение исключительно техники, а не человека. И это тоже часть «технического прогресса», незаслуженно исключенная из рассмотрения философией техники. Ведь внезапное разрушение сложных электронных систем и разветвленных компьютерных сетей, на которых основана современная цивилизация, может привести к коллапсу этой самой цивилизации.

Таким образом, для современного общества чрезвычайно опасными являются не одна, две противоположные тенденции: как бесконтрольное развитие, ведущее к сингулярности, так и все возрастающая опасность внезапного преднамеренного разрушения самой современной техники специальными видами оружия.

1.2. Технический прогресс в релейной защите

Электромеханические реле защиты (ЭМРЗ) на протяжении сотни лет обеспечивали решение всех задач, возникающих в релейной защите, а если учесть, что ЭМРЗ до сих пор составляют во многих странах мира, в том числе и в России, около 70-80% всех типов используемых сегодня защит, то можно с уверенностью заявить, что и сегодня ЭМРЗ в принципе способны решать все задачи, стоящие перед релейной защитой. Тем не менее, в последние 20-25 лет наблюдается повсеместное вытеснение ЭМРЗ микропроцессорными устройствами релейной защиты (МУРЗ). МУРЗ и многочисленные программируемые логические контроллеры (ПЛК), управляющие режимами работы электроэнергетического оборудования, прочно вошли в нашу жизнь и во многих случаях без них уже невозможно обеспечить нормальное функционирование электроэнергетики. И дело здесь не в каких-то особо уникальных возможностях микропроцессорной техники, а в сложившейся тенденции, обусловленной разными причинами, в том числе и сверхприбылью, получаемой при полностью автоматизированном производстве печатных плат МУРЗ по сравнению с производством высокоточной механики реле защиты предыдущего поколения. Поиск путей сокращения производственных затрат и повышения рентабельности производства привел к тому, что 30-40 лет тому назад разработки новых типов

ЭМРЗ были полностью прекращены и все усилия разработчиков были направлены на создание сначала полупроводниковых статических, а затем и микропроцессорных защит. Первые типы МУРЗ попросту копировали все функции и характеристики реле предыдущих поколений. Новые характеристики и возможности у МУРЗ появились лишь много лет спустя. Поэтому вряд ли можно говорить о том, что появление МУРЗ было обусловлено реальными потребностями релейной защиты. В результате такой технической политики производителей, производство всех других типов защит, кроме МУРЗ было полностью прекращено всеми ведущими мировыми производителями релейной защиты и никакой другой альтернативы, кроме МУРЗ, уже практически не осталось (за очень небольшим исключением из этой общемировой тенденции).

Уже самые первые образцы МУРЗ, которые просто копировали функции статических полупроводниковых реле на транзисторах, рис. 1.10, выявили серьезные проблемы МУРЗ: они значительно чаще выходили из строя, их невозможно было ремонтировать из-за наличия специализированного микропроцессора и постоянной памяти с записанной в нее программой. В результате, если реле типа RXIDF-2H на транзисторах и других дискретных компонентах достаточно быстро ремонтировали и возвращали в работу, то их микропроцессорный аналог: RXIDK-2H просто выбрасывали. В результате, микропроцессорные RXIDK-2H уже давно исчезли из эксплуатации, а RXIDF-2H работают до сих пор. Тенденция снижения надежности релейной защиты, связанная с переходом на МУРЗ, замеченная в самом начале этого процесса, прослеживается и до сих пор, несмотря на то, что современные поколения МУРЗ имеют мало общего с самыми первыми образцами, выпущенными несколько десятилетий тому назад, рис. 1.10. Это свидетельствует о том, что проблема заключается не в одиночных технических недоработках ранних образцов МУРЗ, а носит системный характер. Но никто не хотел прослыть ретроградом и никто не хотел говорить об очевидных проблемах, сопровождавших появление МУРЗ, в отношении которых слышны были лишь восторженные отклики. Более того, поскольку за прошедшие годы на развитие идей и технологий, связанных с развитием МУРЗ были истрачены миллиарды долларов и для тысяч ученых и инженеров по всему миру это направление стало весьма прибыльным бизнесом, кормившем их в течение деся-

тилетий, все разговоры о проблемах и недостатках МУРЗ в корне пресекались или встречали яростное неприятие, как представителей предприятий-производителей, так и ученых, разработчиков, проектантов и всех остальных участников этого грандиозного бизнеса. Попытка автора в прошлом обратить внимание на существование проблем с МУРЗ вызывала яростные обвинения в некомпетентности, непонимании основ релейной защиты, и даже в попытке затормозить технический прогресс. В последние годы, правда, появляется осознание существования проблем, но проходит этот процесс как в известном анекдоте: сначала: «этого не может быть потому, что не может быть никогда», потом: «в этом что-то есть» и, наконец: «а разве может быть иначе?», но без средней фазы этого процесса, то есть, без признания правоты того, кто впервые обратил внимание на эти проблемы.

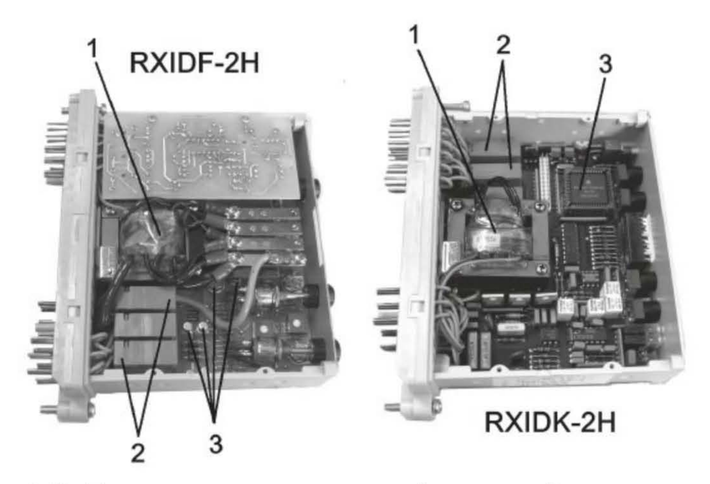


Рис. 1.10. Два токовых реле с зависимой выдержкой времени, с одинаковыми техническими параметрами, характеристиками и размерами, выполненных в одинаковых стандартных корпусах COMBIFLEX® и произведенных одной и той же компанией (ABB), слева – статическое полупроводниковое типа RXIDF-2H, справа - микропроцессорное RXIDK-2H

1 – входной трансформатор тока; 2 – выходные электромагнитные реле; 3 – транзисторы в статическом реле и специализированный микропроцессор – в микропроцессорном

Многочисленные плагиаторы просто копируют целые куски текста из статей и книг автора и включают их в свои статьи без всяких ссылок на первоисточник, докладывают на конференциях, и даже представляют полностью без всяких правок на конкурсы лучших студенческих научных работ [1.12 – 1.19].

1.3. Микропроцессоры – основа современной стадии технического прогресса

Дешевизна и доступность микропроцессоров, промышленных контроллеров и современных электронных компонентов высокой степени интеграции, огромная и все расширяющаяся номенклатура таких компонентов, имеющихся на рынке, чрезвычайно высокая производительность оборудования, предназначенного для автоматической установки и распайки элементов поверхностного монтажа на печатную плату, автоматические системы тестирования готовых печатных плат – все это снимает имевшиеся ранее ограничения на сложность электронных систем и область их применения. В связи с чем, микропроцессоры сегодня можно найти уже повсюду, вплоть до сиденья унитаза, где он измеряет температуру соответствующей части тела и управляет нагревателем воды встроенного душа таким образом, чтобы уравнять ее температуру с температурой упомянутой части тела. Такое быстро расширяющееся применение электронных узлов на основе микропроцессоров во всех областях техники при непрекращающемся их усложнении и является сегодня определяющей тенденцией развития техники. Эту тенденцию принято называть «прогрессом» в развитии техники и технологии. Конечно, есть такие области техники и технологии, в которых без вычислительных операций и без микропроцессоров просто не обойтись и микропроцессорная техника действительно позволила совершить технологический скачек. Однако далеко не во всех случаях применения микропроцессорной техники оно реально обосновано техническими требованиями к изделию, причем количество таких случаев возрастает как снежный ком.

Наблюдая эту тенденцию не со стороны, а, так сказать, изнутри, то есть, занимаясь эксплуатацией и ремонтом сложных электротехнических устройств, промышленного назначения, таких как релейная защита, мощные зарядные устройства, инверторы и конверторы,

источники бесперебойного питания и т. п. начинаешь сомневаться в том, что упомянутая выше тенденция и есть технический прогресс. Почему? Да потому, что наблюдаемый сегодня бум, обусловленный резким усложнением аппаратуры и все расширяющимся применением микропроцессоров во всех областях техники, связан не столько с реальными потребностями, сколько со стремлением производителей превзойти конкурентов любой ценой, создать что-то такое, чего до сих пор никто не создавал, получить сверхприбыль. Само по себе желание создать что-то новое или снизить затраты на производство можно было бы только приветствовать, если бы такая тенденция замены хорошо зарекомендовавших себя безупречной работой в течение десятков лет аналоговых систем на дискретных электронных компонентах микропроцессорными, не приводила к существенному усложнению оборудования, превращению его в неремонтопригодное, снижению его надежности, резкому повышению затрат на поддержание его в работоспособном состоянии, не требовала резкого повышения квалификации обслуживающего персонала. При заказе оборудования все эти проблемы остаются в тени, и сталкиваются с ними лишь с началом эксплуатации оборудования. Это и есть та цена, которую потребителям приходится платить за так называемый «прогресс», то есть бездумное и безответственное усложнение техники, осуществляемое, часто, без всяких на то оснований и лишь в угоду технической моде и погоней производителей за прибылью.

1.4. Smart Grid – опасный вектор «технического прогресса» в энергетике

Не осталось уже, наверное, ни одного средства массовой информации, не написавшего восторженных од в честь так называемых «интеллектуальных сетей» (Smart Grid), выдаваемых за последний писк технической моды, сулящий нам невиданные ранее блага. Только ленивые не говорят нынче о своем вкладе в развитие этого новомодного направления. Оказывается, что не только микропроцессорные счетчики электроэнергии, но даже электропечные трансформаторы, устройства компенсации реактивной мощности, сверхпроводящие силовые кабели и т.д. и т.п. – все это элементы «умной сети», под развитие производства которых нужны деньги.

И вот уже образуются государственные целевые инвестиционные программы, выделяются миллиардные инвестиции и начинает крутиться огромный механизм по «роспилу» средств из государственных бюджетов под направление, которому никто толком даже не может дать четкого и понятного определения [1.20]. Известно, однако, что «умная сеть» предполагает установку микропроцессоров на все без исключения элементы системы производства, распределения и учета электроэнергии и организацию между ними информационных каналов на основе компьютерных сетей, преимущественно беспроводных (Wi-Fi). По идее апологетов Smart Grid энергосистема будущего должна выглядеть как современная навороченная сетевая компьютерная игра с тысячами участников – компонентов электрических сетей. А если добавить сюда еще миллионы квартирных счетчиков электроэнергии, объединенных в общую компьютерную сеть (то есть миллионы потенциальных точек подключения к сети хакеров), то станет еще более понятной вся грандиозность и вся опасность этой затеи, обусловленной резким возрастанием уязвимости электроэнергетической системы к хакерским атакам, компьютерным вирусам и преднамеренным деструктивным дистанционным электромагнитным воздействиям, которые подробно рассматриваются ниже. Электромагнитный импульс высотного ядерного взрыва, произведенного в ближнем космосе над территорией страны, рассматривается сегодня как вполне реальный вариант так называемого «нелетального оружия», способного вывести из строя всю микроэлектронную аппаратуру на территории целой страны, сохранив при этом жизни людей.

Увы, все эти опасности или просто «страшилки», как их пренебрежительно называют некоторые апологеты «технического прогресса» в современном его виде, мало заботят ученых и инженеров, получающих зарплаты из фондов развития «умных сетей». От них часто приходится слышать заявления такого рода: наша задача развивать технический прогресс, а заботиться о защите безопасности национальной электроэнергетики – это прерогатива армии и спецслужб, вот они пусть этим и занимаются. Ущербность такой идеологии очевидна и не требует даже пояснения.

1.5. Опасные тенденции развития устройств релейной защиты

В предыдущих многочисленных публикациях мы уже неоднократно обращали внимание на опасность некоторых тенденций в развитии релейной защиты, усиленно пропагандируемых разработчиками и производителями МУРЗ. Речь идет о следующих тенденциях:

1. Непрерывное усложнение МУРЗ и увеличение концентрации защитных функций в одном терминале [1.21, 1.22, 1.23].
2. Навешивание на МУРЗ несвойственных релейной защите функций, например таких, как мониторинг электрооборудования [1.24, 1.25].
3. Использование в МУРЗ недетерминированной логики, а также, так называемых «упреждающих действий», обуславливающих опасность потери контроля над действиями релейной защиты [1.24, 1.25].
4. Расширение использования в МУРЗ свободно-программируемой логики [1.26], сопровождающееся значительным увеличением процента ошибок персонала и неправильных действий защит.
5. Усложнение проверок исправности и вообще эксплуатации релейной защиты по мере накопления в одной энергосистеме множества типов МУРЗ разных производителей, закупаемых по тендерам и отличающихся между собой как конструкцией, так и программным обеспечением. Отсутствие стандартов, оговаривающих единые универсальные требования к конструкции и к программному обеспечению МУРЗ, увеличивающее интеллектуальную нагрузку на персонал и приводящее к значительным экономическим потерям [1.27]. Эта ситуация усугубляется с каждым годом.
6. Существенное ослабление электромагнитной защищенности релейной защиты и в целом энергосистемы по мере расширения использования МУРЗ [1.28-1.30].
7. Повышение уязвимости энергосистем хакерским атакам по мере расширения применения микропроцессорной техники и при использовании более дешевых сетей Ethernet и Wi-Fi

вместо относительно защищенных оптоэлектронных кабелей в системах релейной защиты [1.31].

Это усложнение, и аппаратное и программное, не прошло даром. Как показано в [1.21 - 1.22, 1.32 – 1.35] переход на МУРЗ уже сегодня сопровождается заметным снижением надежности релейной защиты. Однако, несмотря на это, апологеты микропроцессорной релейной защиты считают, что не следует останавливаться на достигнутом, а нужно и дальше продолжать усложнять МУРЗ, увеличивая количество функций, выполняемых одним терминалом; используя в МУРЗ свободно-программируемую логику; недетерминированную логику на основе теорию нейронных сетей; алгоритмы упреждающего действия; навешивая на МУРЗ функции информационно-измерительных систем и систем мониторинга силового электрооборудования; использования беспроводных каналов связи (Wi-Fi) между реле и т.д. Все эти новые разработки, финансируемые крупными корпорациями, а часто и из государственного бюджета, превратились в огромный бизнес и сегодня никто не хочет быть отлученным от этого сладкого «пирога». Участники этого бизнеса отнюдь не озабочены отдаленными последствиями их деятельности, а стремятся лишь побыстрее «протолкнуть» свои новомодные идеи на рынок.

by Bernd Michael Buchholz, NTB Technoservice, Germany and Christoph Brunner, it4power, Zug, Switzerland

industry reports

and prosperity of the industry was clearly considered by Madame Merce Griera I Fisa from the European Commission. The SmartGrids are a prerequisite to reach the European 20-20-20 targets in 2020 (*20% improvement of energy efficiency, 20 % share of renewable energy sources to cover the demand of primary energy, 20 % reduction of carbon emissions*). Furthermore, the advanced products and system solutions partly resulting from funded projects will ensure success of the European industries

presented by the 12 participating project teams – beginning with the building automation "SmartHome" and the involvement of household consumers into the electricity market, the automation of distribution networks up to the erection of prospective markets for energy and reserve power. Engaged discussions followed each of the contributions.

The analysis of the consumer behavior in the environment of dynamic tariffs presented a potential of 14% energy saving and load

It is mandatory that the new solutions from the project are urgently applied in practice now.

One session considered the barriers for SmartGrid solutions by the current regulation and legal situation in Germany. For many

Рис. 1.11. Девиз к одной из публикаций в популярном среди специалистов во всем мире журнале “Protection, Automation and Control Magazine” – PAC World, September, 2011 (выделенный рамкой), который можно перевести как: «немедленное внедрение новых разработок сегодня должно стать обязательной практикой»

Бизнес – есть бизнес и его основополагающие законы действуют одинаково во всех странах и во всех областях, включая такую чувствительную область, как релейная защита, системы управления и контроля в электроэнергетике. Не верите? Тогда познакомьтесь с девизом к отчету о симпозиуме “Distribution systems of the future: Novel ICT solutions as the backbone for smart distribution”, опубликованному в журнале PAC World, рис. 1.11. Ключевые слова здесь: «немедленно» и «обязательно», то есть без тщательного анализа отдаленных последствий этих нововведений и без никому не нужной критики. Так действовали до недавнего времени во всех странах мира.

Однако, после периода весьма бурной критической реакции на публикации автора и полного отрицания негативных последствий перечисленных выше тенденций в развитии релейной защиты, в последние годы появляется понимание сформулированных нами ранее проблем многими специалистами. Так, например, B. Morris, R. Moxley, C. Kusch (Schweitzer Engineering Laboratories, США) представили доклад: «Then Versus Now: A Comparison of Total Scheme Complexity» на Второй Международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем» (Москва, 7–10 сентября 2009 г.), в котором они ставят под сомнение необходимость всё большего усложнения защит, аргументируя это сравнительными оценками надежности защит на основе простых электромеханических реле и многофункциональных микропроцессорных систем защиты. Они заявили о выявленной ими тенденции снижения надежности систем релейной защиты, построенных на основе всё более усложняющихся микропроцессорных устройств. О недостаточной надежности МУРЗ заявил также В.И. Пуляев (ФСК ЕЭС, Россия) на Третьей Международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем» (Санкт-Петербург, 30 мая - 3 июня 2011 г.). Он отметил, в частности, что значительная доля сбоев релейной защиты приходится на микропроцессорные устройства (примерно 23% из всех случаев), которые составляют всего около 10% от общего количества устройств защиты. Это, безусловно, один из важнейших факторов, определяющих необходимость принятия специальных мер по повышению надежности МУРЗ. Ныне покойный Алексей Шалин (д.т.н., профессор кафедры

электрических станций Новосибирского государственного технического университета, ведущий специалист ООО «ПНП БОЛИД», г. Новосибирск) прямо писал в своей статье-отзыве на одну из наших публикаций (см. А. Шалин «Микропроцессорные реле защиты: необходим анализ эффективности и надежности», ж. «Новости электротехники», 2006, № 2) о том, что процент неправильных действий современных панелей и шкафов РЗ часто оказывается существенно выше, чем для старых защит, выполненных на электромеханических реле и том, что статистические данные подтверждают факт существенного снижения эффективности и надежности при переходе от защит, выполненных на электромеханических реле, к микропроцессорным терминалам. О проблемах с надежностью современных МУРЗ писали А. Н. Владимиров (Центральное диспетчерское управление ЕЭС России); S. Swain, D. B. Ghosh (Integrated Electrical Maintenance) и др. [1.36]

Stokoe J. и Gray. J. в своем докладе “Development of a Strategy for the Integration of Protection & Control Equipment» на 7 Международной конференции «Developments in Power Systems Protection» (Amsterdam, 9-12-th April 2001) отмечал, что старые электромеханические реле были прочными и долговечными устройствами со сроком службы 25 лет, тогда как срок службы современных микропроцессорных защит составляет 15 лет и менее. Им вторят J. Polimac и A. Rahim (PB Power, United Kingdom), утверждающие, что при переходе от электромеханических реле к микропроцессорным, срок службы защит уменьшился с 40 лет (для электромеханики) до 15-20, а иногда и вообще до нескольких лет после введения в эксплуатацию (для МУРЗ) [1.36].

Руководитель компьютерного отделения Инженерно-технологического колледжа (University of Poona, Maharashtra, India) Ashok Kumar Tiwari B. E. отмечает, что объединение в одном микропроцессорном терминале множества функций резко снижает надежность релейной защиты, поскольку при отказе этого терминала будет утеряно сразу слишком много функций по сравнению со случаем, когда эти функции распределены среди нескольких терминалов [1.36]. О необходимости ограничении количества функций, реализуемых в одном терминале МУРЗ, говорили также в своем докладе на упомянутой выше Третьей Международной конференции «Современные направления развития систем релейной защиты

и автоматики энергосистем» В. А. Ефремов и С. В. Иванов (ИЦ «Бреслер»), Д. В. Шабанов (ФСК ЕЭС России).

А. Федосов и Е. Пусенков, (филиал ОАО "СО ЕЭС" ОДУ Сибири) в своей статье «Проблемы, возникающие при внедрении микропроцессорной техники в системах противоаварийной автоматики» (ж. «Электрические станции», 2009, № 12) отмечают отсутствие универсальных жестких требований к аппаратной части МУРЗ и к программному обеспечению и, вследствие этого, слишком большое многообразие программ и алгоритмов, заложенных в МУРЗ, используемых в одной энергосистеме, что приводит к проблемам при эксплуатации и к увеличению вероятности ложной работы данных устройств. О резком повышении уровня сложности работ персонала, обслуживающего релейную защиту с переходом от электромеханики к МУРЗ – как о причине тяжелых аварий в энергосистемах писали также D. Rayworth и M. A. Rahim (PB Power, UK) [1.36]. О сложности программного интерфейса и необходимости введения чрезмерного количества уставок при программировании МУРЗ писали А. Беляев, В. Широков и А. Емельянцев (Специализированное управление «Леноргэнергогаз», г. Санкт-Петербург) в своей статье: "Цифровые терминалы РЗА. Опыт адаптации к российским условиям" (ж. Новости электротехники, 2009, № 5).

О неудовлетворительном состоянии электромагнитной обстановки на большинстве старых подстанций, которые проектировались и строились под электромеханическую релейную защиту, а не под микропроцессорную и о возникающих из-за этого многочисленных сбоев в работе МУРЗ, отмечали Ковалев Б.И., Наумкин И.Е. (Сибирский НИИ энергетики); Бордачев А. М. (ОАО «Институт Энергосетьпроект»); М. Матвеев и М. Кузнецов (ООО «ЭЗОП»); P. Montignies, B. Jover (Schneider Electric, France); В. Надеин («Архэнерго»); В. Лопухов (ГУП «ПЭО Татэнерго»); А. Ермишкин (АО «Мосэнерго»); Р. Борисов (НПФ «ЭЛНАП», г. Москва); A. W. Sowa, J. Wiater (Electrical Department, Białystok Technical University, Poland) и другие специалисты. Многие из них отмечали, что чувствительность к электромагнитным помехам устройств релейной защиты на микропроцессорной элементной базе на несколько порядков выше, чем у их традиционных электромеханических аналогов и поэтому для обеспечения электромагнитной совместимости (ЭМС) вторичных цепей необходимо резко по-

высить уровень их электромагнитной защиты. Без проведения комплекса работ по обеспечению ЭМС невозможно достигнуть приемлемых характеристик надежности МУРЗ.

С проблемой низкой устойчивости МУРЗ к электромагнитным помехам тесно связана еще более сложная и тяжелая проблема преднамеренных дистанционных деструктивных воздействий (ПЭДВ) на МУРЗ, на которую мы впервые обратили внимание специалистов в [1.36]. Сегодня во многих странах мира уже разработана аппаратура, способная дистанционно вывести из строя любые микропроцессорные системы промышленного назначения (включая и МУРЗ, естественно) поэтому этой проблеме посвящены не только многочисленные публикации в технических журналах таких известных специалистов, как Manuel. W. Wik (Defence Materiel Administration, Sweden) и William A. Radasky (Metatech Corporation, USA), но также и отчеты специальных комиссий при Конгрессе США (см., например: «Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack», 2008).

Еще одной новой проблемой, неизвестной ранее в релейной защите, является проблема кибернетической уязвимости МУРЗ (а, следовательно, и в целом энергосистемы) к хакерским атакам. Парализация систем управления, масштабные отключения целых энергосистем, хаос в системах контроля, отключение интернета и сотовой связи – так, по мнению американских апологетов выглядит сценарий последствий кибернетической атаки. Причем, учитывая стратегическую важность такого объекта, как энергосистемы, заниматься такими атаками будут уже не хакеры-одиночки, а специальные военные кибернетические подразделения, уже созданные во многих странах мира. Буквально в прошлом году при Агентстве Национальной Безопасности США – одной из самых могущественных и засекреченных спецслужб мира, возглавляемой генералом К. Александером было создано отдельное Киберкомандование, объединившее все существовавшие ранее подразделения киберзащиты Пентагона. Часть из них будут обеспечивать безопасность не только военной и государственной инфраструктуры, но и наиболее важных коммерческих объектов страны. Понятно, что такая огромная структура будет заниматься не только защитой от хакерских атак, но и разработкой самих атак (лучшая защита – нападение). Нынешний глава Киберкомандования, он же директор АНБ генерал К.

Александер заявил на слушаниях Комитета по делам Вооруженных Сил США Палаты Представителей Конгресса, что кибероружие имеет эффект, сравнимый с эффектом применения оружия массового уничтожения. Кибероружие развивается с большой скоростью. Многие страны - включая США, Россию, Китай, Израиль, Великобританию, Пакистан, Индию, Северную и Южную Корею - развили сложное кибероружие, которое может неоднократно проникать в компьютерные сети и способно разрушать их, утверждают специалисты по кибербезопасности. В 2010 г. кибербюджет США составил 8 млрд. долларов и в последующем он будет только возрастать. В 2011 году США планировали принять новую доктрину кибербезопасности. О ее направленности можно судить по опубликованной программной статье заместителя главы Пентагона Уильяма Линна III с символичным названием «Защищая новое пространство». Ее главная мысль: отныне США будут считать киберпространство таким же потенциальным полем боя, как сушу, море и воздух. Параллельно над созданием концепции коллективной кибербороны начали работать и в НАТО. На ноябрьском 2010 г. саммите альянса было решено разработать «План действий в области кибербороны». Документ должен был быть подготовлен к апрелю 2011 г., а подписан в июне. Важное место в нем отведено созданию центра НАТО по реагированию на киберинциденты. Изначально его предполагалось запустить в 2015 году, но по настоянию США срок сократили на три года. Об эффективности кибероружия можно судить по широко известной кибератаке Иранского центра по обогащению урана в Натанзе с помощью компьютерного червя Win32/Stuxnet, разрушившего сотни центрифуг. Еще одна массированная атака на Японскую корпорацию Mitsubishi Heavy Industries, занимающуюся производством самолетов F-15, ракетно-зенитных комплексов Patriot, подводных лодок, надводных кораблей, ракетных двигателей, системами наведения и перехвата баллистических ракет и другой военной техникой, произошла в сентябре 2011 г. Компьютерное оборудовании корпорации (45 закрытых серверов и около 50 персональных компьютеров) оказалось заражено целым набором вирусов, которые полностью взяли их под свой контроль. Они позволяли управлять компьютерами со стороны, перемещать имеющуюся на них информацию. Были и вирусы, которые давали возможность активизировать встроенные в компьютеры микрофоны и камеры. Это

позволяло злоумышленникам на расстоянии следить за происходящим в рабочих и исследовательских помещениях. Некоторые вирусы стирали следы взлома, что серьезно затрудняет оценку масштабов ущерба. Информация с взятых под контроль компьютеров перекачивалась на 14 сайтов за границей, в том числе на территории Китая, Гонконга, США, Индии.

Современные технологии позволяют запускать в компьютерную систему вирусы дистанционно в виде кодированного радиоизлучения с помощью беспилотных летательных аппаратов-ретрансляторов. Особенно уязвимы к таким проникновениям извне беспроводные системы Wi-Fi, на основе которых и планируется создание систем Smart Grid. Встроенными модемами для Wi-Fi уже сегодня снабжаются МУРЗ ведущих Западных производителей.

В прошлом уже были зарегистрированы неоднократные попытки компьютерного проникновения в энергосистему Израиля, предпринятые Ираном. Старший аналитик ЦРУ США Tom Donahue заявил на встрече правительственных чиновников и сотрудников американских компаний, владеющих системами электро-, водо-, нефте- и газоснабжения об известных ЦРУ многочисленных попытках проникновения в энергосистемы США.

Совершенно очевидно, что перечисленные выше тенденции будут лишь усиливаться по мере развития технологий, если не будут приняты специальные меры, предотвращающие эти тенденции:

1. В области надежности РЗ:

1.1 Введение в практику уточненных методов расчета надежности МУРЗ [1.37] и нового показателя надежности [1.38] – удобного и практичного, позволяющего потребителю предъявлять претензии производителю вместо применяющегося сегодня малоинформативного показателя «наработка на отказ» (MTBF).

1.2 Ограничение и оптимизация количества функций в одном модуле МУРЗ [1.39,1.40].

1.3 Отказ от использования в МУРЗ недетерминированной логики [1.24, 1.25, 1.41].

1.4 Существенное ограничение использования в МУРЗ свободно-программируемой логики – источника ошибок персона-

ла и большого количества неправильных действий РЗ [1.24, 1.25, 1.41].

1.5 Введение запрета на использование МУРЗ для целей, не имеющих прямого отношения к релейной защите, например, для мониторинга состояния электрооборудования или для так называемых «защит упреждающего действия» [1.24, 1.25, 1.41].

1.6 Отказ от использования в РЗ беспроводных сетевых технологий.

1.7 Обязать в законодательном порядке производителей МУРЗ заботиться о кибербезопасности и устойчивости к преднамеренным электромагнитным деструктивным воздействиям (ПЭДВ) выпускаемой ими продукции. Для чего разработать нормы и ввести в техническую документацию на МУРЗ специальные разделы, в которых должны быть отражены предпринятые меры, степени защиты данного конкретного МУРЗ от вышеуказанных воздействий и соответствие их установленным нормам. Постепенно ввести ограничения, а затем и полный запрет на использование в электроэнергетике МУРЗ, не отвечающих требованиям защищенности от указанных воздействий.

1.8 Выпустить специальные бюллетени для проектных организаций, занятых проектированием систем релейной защиты, с подробным описанием существующих сегодня опасностей для РЗ и возможных мер защиты от них [1.11]. Постепенно применять в практике проектирования известные нормы и меры защиты сначала на вновь вводимых энергообъектах, а потом и на существующих.

1.9 Поручить ведущим научным организациям разработку конкретных программных и аппаратных средств защиты от вышеуказанных воздействий, а также тестирование, организацию опытной эксплуатации и последующего производства уже известных эффективных и, вместе с тем, сравнительно недорогих аппаратных средств защиты, предложенных в [1.42 – 1.43, 1.11].

2. *В области стандартизации РЗ*

2.1 Ввести в нормативно-техническую документацию единые определения для важнейших понятий релейной защиты, например, предложенные в [1.44].
2.2 Переработать общие технические требования к микропроцессорным устройствам защиты и автоматики энергосистем (РД 34.35.310-97) на основе международных стандартов, и выпустить новый документ, взяв за основу требования, изложенные, например, в [1.44].
2.3 Унифицировать конструкцию и базовую программную оболочку МУРЗ различных типов и производителей, для чего разработать набор стандартов с едиными техническими требованиями к конструктивному исполнению функциональных модулей МУРЗ, к внутренним протоколам связи между ними, к базовой пользовательской программной оболочке [1.44].
2.4 Стандартизировать испытания МУРЗ с использованием современных программируемых тестовых систем релейной защиты и пакетов готовых программных модулей [1.44].

Предложенные меры, по нашему мнению, способны остановить дальнейшее развитие опасных тенденций области МУРЗ и будут способствовать значительному увеличению надежности РЗ, ее устойчивости к различным видам преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) и снижению затрат на ее эксплуатацию.

Литература к Гл. 1.

1.1 Попкова Н. В. Философия техники. – Интернет-портал Брянского отделения Российского философского общества (http://sphil.iipo.tu-bryansk.ru/)
1.2 Vinge V. The coming technological singularity: How to survive in the post-human era. - NASA. Lewis Research Center, Vision 21: Interdisciplinary Science and Engineering in the Era of Cyberspace pp. 11-22 (SEE N94-27358 07-12), 12/1993.

1.3 Moore G. E. Cramming More Components onto Integrated Circuits. – "Electronics", April 19, 1965, pp. 114–117.

1.4 Сухарев М. Взрыв сложности. - "Компьютерра", № 43, 03 ноября 1998 года (http://offline.computerra.ru/1998/271/1828/).

1.5 Негодаев И. А. Философия техники: Учеб. пособие / ДГТУ (учеб. пособие) /Ростов н/Д, 1998, 319 с.

1.6 В.А. Лопота, Е.И. Юревич. Унифицированные микросистемные мехатронные модули – основа интеллектуальной техники будущего. - Искусственный интеллект, 2002, № 3, с. 303 – 304.

1.7 Безменов А. Е. Допуски, посадки и технические измерения. Учебник для техникумов. Москва: Машиностроение, 1969, 322 с.

1.8 Гуревич В. И. Микропроцессорные реле защиты. Устройство, проблемы и перспективы. – М.: Инфра-Инженерия, 2011. – 336 с.

1.9 Буренок В. М. Как обеспечить обороноспособность России в будущем? – Военно-промышленный курьер, вып. № 39 (507), 9 октября 2013 г.

1.10 Гиндилис Л. М. Модели цивилизаций в проблеме SETI. – Общественные науки и современность, 2000, № 1, с. 115 – 123.

1.11 Гуревич В. И. Уязвимости микропроцессорных реле защиты: проблемы и решения. – М.: Инфра-Инженерия, 2014. – 256 с.

1.12 Грищук Ю.С., Тимошенко Р.Ф. Аналіз надійності мікропроцесорних пристроїв релейного захисту // Сборник научных трудов "Вестник НТУ "ХПИ": Проблеми вдосконалення електричних машин і апаратів, № 16 - Вестник НТУ "ХПИ", 2010.

1.13 Внуков А. А. Опыт внедрения микропроцессорных терминалов в современных условиях. – Электро. Электротехника, электроэнергетика, электротехническая промышленность, 2008, №1, с. 40-41.

1.14 Сапа В. Ю. Электромагнитная совместимости в современной электроэнергетике. - Материалы конференции «Достижения высшей школы. Технические науки» (Костанайский государ-

ственный университет им. А. Байтурсынова), Казахстан, 2011.

1.15 Арынов А. К., Юнус М.Э. Сравнительный анализ цифровых устройств релейной защиты. – Вестник Казахского национального технического университета им. К. И. Сатпаева, 2011, № 1(83).

1.16 Линт М. Г., Матисон В. А., Михайлов А. В. Современное состояние и перспективы электромеханических устройств РЗА. – Релейная защита и автоматизация, 2013, № 2, с. 38 – 40.

1.17 Колесник С. П. Стратегическое направление завода-устройства и реле для энергетики. – Тезисы доклада на семинаре «Устройства релейной защиты и автоматики производства ОАО «Электротехнический завод». Опыт внедрения и применения», Релсіс, Киев, 2007.

1.18 Гребенников М. Определяя верное направление. - Энергетика и промышленность России, № 18 (134) сентябрь 2009г.

1.19 Иов А. А и Иов И. А. Надежность микропроцессорных устройств релейной защиты: мифы и реальность. – Секция «Электроснабжение и системы управления электрооборудованием горных предприятий». Всероссийская научно-практическая конференция "Инновационное развитие горно-металлургической отрасли», Иркутский государственный технический университет, Иркутск, 1-2 декабря 2009 г.

1.20 Гуревич В. И. Интеллектуальные сети: новые перспективы или новые проблемы? - Электротехнический рынок, 2010, № 6 (часть 1); 2011, № 1 (часть 2).

1.21 Гуревич В. И. Надежность микропроцессорных устройств релейной защиты: мифы и реальность. - Проблемы энергетики, 2008, № 5 - 6, с. 47 - 62.

1.22 Гуревич В. И. Еще раз о надежности микропроцессорных устройств релейной защиты. - Электротехнический рынок, 2009, № 3 (29), с. 40 - 45.

1.23 Гуревич В. И. Энергобезопасна ли релейная защита? - Энергобезопасность и Энергосбережение, 2010, № 2, с. 6 - 8.

1.24 Гуревич В. И. "Интеллектуализация" релейной защиты: благие намерения или дорога в ад? - Электрические сети и системы, 2010, № 5, с. 63- 67.

1.25 Гуревич В. И. Сенсационные открытия в области релейной защиты. - Энергетика и промышленность России, 2009, № 23-24, с. 60.

1.26 Гуревич В. И. Логика в свободном полете. - PRO Электричество, 2011, №2, с. 28 - 31.

1.27 Гуревич В. И. Испытания микропроцессорных реле защиты. - PRO Электричество, 2008, № 1 (25), с. 41 - 43.

1.28 Гуревич В.И. Электромагнитный терроризм - новая реальность 21 века. – Мир техники и технологий, 2005, N. 12, с. 14 – 15.

1.29 Гуревич В. И. Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. - Компоненты и технологии, 2010, № 2, с. 60-64; № 3, с. 91-96; № 4, с. 46-51.

1.30 Гуревич В. И. Проблема устойчивости микропроцессорных систем релейной защиты и автоматики к преднамеренным деструктивным электромагнитным воздействиям. - Компоненты и технологии, 2011, № 4 (часть 1); 2011, № 5 (часть 2).

1.31 Гуревич В. И. Кибероружие против энергетики. - PRO Электричество, 2011, №1, с. 26 - 29.

1.32 Гуревич В. И. Микропроцессорные реле защиты: новые перспективы или новые проблемы? - Новости электротехники, 2005, № 6 (36), с. 57 - 60.

1.33 Гуревич В. И. О некоторых оценках эффективности и надежности микропроцессорных устройств релейной защиты. - Вести в электроэнергетике, 2009, № 5, с. 29 - 32.

1.34 Гуревич В. И. Актуальные проблемы релейной защиты: альтернативный взгляд. - Вести в электроэнергетике, 2010, № 3, с. 30 - 43.

1.35 Гуревич В. И. Критерии оценки релейной защиты: следует ли усложнять ситуацию? - Вести в электроэнергетике, 2009, № 6, с. 45 - 48.

1.36 Проблемы микропроцессорных устройств релейной защиты - http://digital-relay-problems.tripod.com

1.37 Гуревич В. И. Проблемы оценки надежности релейной защиты. – Электричество, 2011, № 2, с. 28 – 31.

1.38 Гуревич В. И. Для оценки надежности микропроцессорных устройств релейной защиты нужен новый критерий. - Электротехнический рынок, 2011, № 6, с. 70 - 74.
1.39 Гуревич В. И. Актуальные проблемы стандартизации в области релейной защиты. – Вести в электроэнергетике, 2012, № 6, с. 28 – 38.
1.40 Гуревич В. И. Про многофункциональную релейную защиту. - "PRO Электричество", 2012, № 42-43, с. 45 - 48.
1.41 Гуревич В. И. Сюрреализм в релейной защите. - ЭнергоStyle, 2010, № 1, с. 5 - 7.
1.42 Гуревич В. И. Нужна ли защита релейной защите? - Электроэнергия. Передача и распределение, 2013, № 2, с. 94-97.
1.43 Гуревич В. И. Устройство защиты релейной защиты. - Компоненты и технологии, 2013, № 5.
1.44 Гуревич В. И. Проблемы стандартизации в релейной защите. – СПб.: Издательство ДЕАН, 2015. – 168 с.

2. ПРЕДНАМЕРЕННЫЕ ДЕСТРУКТИВНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ВОЗДЕЙСТВИЯ

2.1 Введение

Применение специального оружия, способного разрушить систему электроснабжения и другие важнейшие элементы национальной инфраструктуры, не воздействуя напрямую на человека, является весьма заманчивым, поскольку может привести к коллапсу целой страны, притом, что лиц, ответственных за принятие решения о применении такого оружия, никто не сможет осудить за массовое убийство гражданского населения, поскольку это оружие не имеет прямого воздействия на людей. Таким оружием являются системы, генерирующие сверхмощные электромагнитные поля, выводящие из строя электронную аппаратуру и электротехническое оборудование.

Проблема преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электроэнергетические системы становится в последнее время все более актуальной в связи с двумя современными тенденциями: расширяющимся применением микроэлектроники и микропроцессорной техники в электроэнергетике - с одной стороны, и интенсивными разработками средств дистанционного поражения электронной аппаратуры – с другой [1]. Причем, проблема эта касается не только такой сугубо гражданской отрасли, как электроэнергетика, но и военных, поскольку военные базы и полигоны получают электроэнергию и воду от гражданских систем и серьезные сбои в функционировании этих систем неминуемо скажутся на боеготовности армии со всеми ее системами вооружения, защищенными от ПЭДВ.

2.2 Краткий исторический экскурс

Разрушительное влияние удаленного ядерного взрыва на электронную аппаратуру было обнаружено при первых же испытаниях этого нового в то время вида оружия. Теоретическое обоснование феномена образования мощного электромагнитного импульса при ядерном взрыве (ЭМИ ЯВ) было в последствие найдено в тео-

ретических трудах лауреата Нобелевской премии в области физики Артура Комптона, выполненных им еще в 1922 году. Военные быстро оценили перспективы применения этого феномена в качестве оружия, поражающего инфраструктуру противника, в первую очередь, системы электроснабжения. Первые прямые эксперименты по изучению ЭМИ ЯВ были проведены 9 июля 1962 г. Комиссией по атомной энергии и Агентством по ядерной безопасности Министерства обороны США (проект под шифром «Starfish Prime» - «Первая морская звезда»). Ракета с термоядерной боеголовкой мощностью 1.44 мегатонны была запущена с военного полигона США, расположенного на аттоле Джонстон (Johnston Attol) между Маршалловыми и Гавайскими островами в Тихом океане на высоту около 450 км и там подорвана. Это испытание было лишь одним из пяти высотных ядерных взрывов, направленных на изучение ЭМИ ЯВ, проведенных США в 1962 г. в рамках более обширного проекта под шифром «Operation Fishbowl» («Аквариум»). При проведении этих испытаний были зафиксированы мощные электромагнитные импульсы, которые обладали большим поражающим действием на электронную аппаратуру, линии связи и электроснабжения, радио- и радиолокационные станции и даже вывели из строя уличное освещение на Гавайях, на расстояниях около полутора тысяч километров от эпицентра взрыва [2].

В том же 1962 году (22 октября, 28 октября и 1 ноября) в Советском Союзе в рамках так называемого «Проекта К» была произведена серия из трех высотных ядерных взрывов, каждый мощностью в 300 кт (К3-184; К4-187 и К5-195), направленных на изучение явления ЭМИ ЯВ. Ракеты с ядерными боеголовками запускались с ракетного полигона Капустин Яр в Астраханской области и подрывались на высотах 60 – 290 км над территорией военного полигона в Сары-Шаган, Карагандинской обл. в Казахстане (Закрытое административно-территориальное образование Приозерск). Работы по исследованию ЭМИ ЯВ и подготовке этих испытательных ядерных взрывов проводились в СССР Центральным физико-техническим институтом Министерства обороны (в/ч 51105 или ЦНИИ-12) в Сергиевом Посаде Московской обл. (ныне ФГУ "12 ЦНИИ МО РФ"). Во время одного из тестов (К3-184) были зафиксированы импульсные токи до 3400 А в проводах воздушных телефонных линий, которые обусловили появление импульсного напряжения с ам-

плитудой до 28 кВ, срабатывание всех установленных в аппаратуре разрядников и перегорание всех предохранителей, что сопровождалось прекращением работы системы связи, зафиксировано повреждение систем радиосвязи на расстоянии 600 км от эпицентра взрыва, выход из строя радиолокатора, расположенного на расстоянии 1000 км, повреждения трансформаторов и генераторов на электростанциях, пробои изоляторов ЛЭП, рис. 2.1. Серьезные повреждения аппаратуры были зафиксированы и на космодроме Байконур. Причем, речь идет об аппаратуре поколения 60-х годов, выполненной на электромеханических элементах и на радиолампах, на порядки более устойчивых к воздействию ПЭДВ, чем современная микроэлектронная и микропроцессорная техника.

Рис. 2.1. Иллюстраций повреждений оборудования, подвергшегося воздействию высотного ЭМИ ЯВ над Казахстаном в 1962 г. Впервые рисунок был представлен на англ. языке начальником ЦНИИ-12 генерал-майором, д.т.н, профессором В. М. Лоборевым, на международной конференции EUROEM во Франции в 1994 г. [3]

Кроме того, и в американских и в советских опытах использовались термоядерные заряды, электромагнитный импульс которых, как оказалось, в 3-5 раз слабее импульса возникающего при детонации обычного ядерного заряда такой же мощности.

2.3 Первая открытая достоверная информация об ЭМИ ЯВ и методах защиты в электроэнергетике

Совершенно естественно, что в связи со сложностью, важностью и высокой стоимостью проведения испытательных ядерных взрывов, вся информация о них была тщательно засекречена и что первыми обладателями такой информации были военные специалисты. Можно было бы предположить, что первой открытой информацией такого рода была информация, представленная во времена «перестройки» начальником Центрального физико-технического института Министерства обороны генерал-майором В. М. Лоборевым, в его знаменитом докладе на конференции EUROEM во Франции в 1994 г. Но на самом деле это совсем не так. Оказывается, первые публикации в открытой печати подробных и достоверных сведений о параметрах ЭМИ ЯВ и о его влиянии на инфраструктуру страны, в частности, на системы электроснабжения, относятся к концу 60-х – началу 70-х годов прошлого века, то есть, все эти сведения находятся в открытом доступе уже 40-50 лет [4 - 23]. Причем, в некоторых из этих публикаций (например, в [16, 18]) содержится подробное описание также и средств защиты электрооборудования от воздействия ЭМИ ЯВ. Как можно видеть, большинство этих работ опубликовано в США, поэтому было бы логично предположить, что за прошедшие полвека США добились непревзойденных успехов в области защиты важнейших составных частей своей национальной инфраструктуры от ЭМИ ЯВ. Тем более, что в этом должна быть заинтересована и армия.

2.4 Реальное положение дел с защитой систем электроснабжения от ЭМИ ЯВ и других видов ПЭДВ

«Вы можете дурачить всех людей некоторое время;
можете даже все время дурачить некоторых людей;
но вам никогда не удастся дурачить всех людей все время».

/Авраам Линкольн/

Что же реально происходит в США и в мире в деле защиты электроэнергетики и других важнейших систем, образующих ин-

фраструктуру страны, от воздействия ПЭДВ? Наверное, очень многое, если судить по количеству государственных и частных структур занимающихся этой проблемой и финансируемых из госбюджета страны, хотя бы в одних только в США. Вот перечень лишь некоторых из них:

- Metatech Corp.
- Department of Homeland Security (DHS)
- EMP Commission of Congress
- North American Electric Reliability Corp. (NERC)
- Department of Energy
- Department of Defense (DoD)
- Critical Infrastructure Partnership Advisory Council (CIPAC)
- Electric Infrastructure Security Council (EICS)
- Defense Science Board (DSB)
- US Strategic Command (USSTRATCOM)
- Defense Threat Reduction Agency (DTRA)
- Defense Logistics Agency (DLA)
- Air Force Weapons Laboratory
- FBI
- Sandia National Laboratories
- Lawrence Livermore National Laboratory (LINL)
- Oak Ridge National Laboratory
- Idaho National Laboratories
- Los Alamos National Laboratories
- Martin Marietta Energy Systems, Inc.
- National Security Telecommunications Advisory Committee
- Federal Emergency Management Agency (FEMA)
- National Academy of Science
- Task Force on National and Homeland Security
- EMPrimus
- Neighborhood of Alternative Homes (NOAH)
- EMPact America
- Federal Energy Regulatory Commission (FERC)
- Electric Power Research Institute (EPRI)
- NASA
- U.S. Northern Command (NORTHCOM)
- SHIELD Act

- EMP Grid
- EMP Technology Holding
- Strategic National Risk Assessment (SNRA)
- Walpole Fire Department

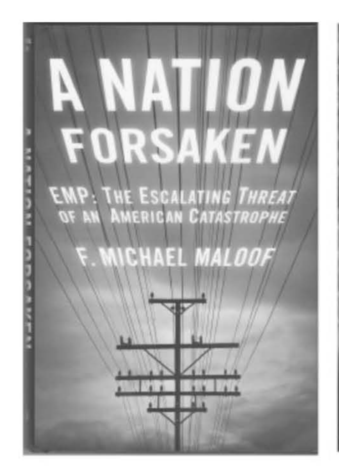
Международные организации с участием США:
- International Electrotechnical Commision (IEC), Technical Subcommittee 77C
- CIGRE, Working Group WG C4.206

Уважаемый читатель, не кажется ли тебе несколько подозрительным активное участие такого большого количества организаций всего лишь в одной стране в теме, по которой за прошедшие десятилетия опубликовано огромное количество материалов и фактически не осталось уже ни одного «белого пятна», которое требовало бы дальнейших исследований?

Оказалось, что тема ПЭДВ и, в частности, ЭМИ ЯВ – не что иное, как прекрасный «долгоиграющий» инструмент для «распиливания» государственного бюджета. И, похоже, никто не заинтересован в том, чтобы процесс «роспила» наконец завершился какими-то конкретными действиями по защите систем электроснабжения. В подтверждение этому приведем высказывание одного из бывших чиновников Министерства обороны США Эштона Картера (Dr. Ashton Carter): «*Армия, флот и Стратегическое командование продолжают думать над тем, чтобы подумать о проблеме*». Более определенно на эту тему высказался исполнительный директор Организации по национальной безопасности (Task Force on National and Homeland Security) д-р Питер Винсент Прай (Peter Vincent Pry): «*Проблема не в технологиях. Мы знаем, как защититься от этого. Проблема не в деньгах, это стоит не так уж дорого. Проблема в политике. Как всегда появляется политика, которая мешает делу*».

В своей большой книге под названием «Неизвестный Апокалипсис», рис. 2, д-р Прай сетует на то, что в некоторых других странах (Израиле, Англии, России) дело обстоит намного лучше, чем в США и там уже приступили к реализации практических шагов по защите электрических систем. Поспешим успокоить д-ра Прайа: он может не переживать за отставание США. На самом деле ситуация в этой области, например, в России намного хуже чем в

США, поскольку там специалисты в области электроэнергетики или вообще ничего не слышали об этой проблеме, или считают ее «страшилками Гуревича» (поскольку единственным автором, пишущим на эту тему в русскоязычных изданиях, является автор данной книги). Не лучше обстоит дело и в других странах. В общем, становится понятным, почему на протяжении десятков лет нигде в мире не делается абсолютно ничего конкретного по защите электроэнергетики от ПЭДВ и все ограничивается лишь многостраничными отчетами об исследованиях, докладами, семинарами, конференциями и другими видами приятного времяпровождения в кругу коллег. Просто многочисленные «участники процесса» вовсе не заинтересованы в окончании многолетнего процесса исследований, а заинтересованы в поддержании этой темы «на плаву» и продолжении финансирования ее.



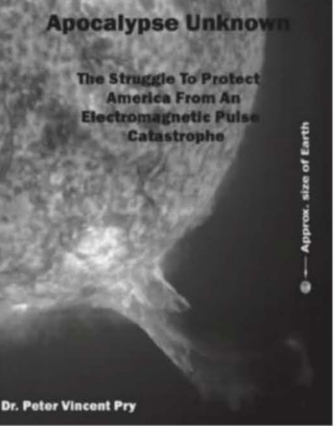


Рис. 2.2. Книга Михаила Малоофа «Нация, брошенная на произвол судьбы», посвященная описанию бюрократических и политических игр в США по проблеме ПЭДВ (слева) и книга Питера Винсента Прайа «Неизвестный апокалипсис» (справа)

Этой проблеме посвящена целая книга бывшего аналитика Пентагона Михаила Малоофа (Michael Maloof): «Нация, брошенная на произвол судьбы», рис. 2.2. О серьезных бюрократических препо-

нах в этом деле пишет в своей книге «Apocalypse Unknown" ("Неизвестный апокалипсис») также упомянутый выше Питер Винсент Прай.

Свою лепту в затягивание процесса реализации хорошо известных конкретных мер по защите систем электроснабжения от ПЭДВ вносят и представители могущественного военно-промышленного комплекса (ВПК). Они настаивают на том, что единственной эффективной защитой против ЭМИ ЯВ является национальная система противоракетной обороны (ПРО), в которую нужно вкладывать побольше бюджетных средств. Такая позиция представителей ВПК становится вполне понятной, если сравнить относительно небольшую стоимость средств защиты важнейших частей и систем инфраструктуры страны от ЭМИ ЯВ со стоимостью разработки и производства эффективного многоярусного противоракетного щита, защищающего все страну. Ну, а что касается других, не ядерных средств ПЭДВ [1], то поскольку системы ПРО не защищают от них, то следует сделать вид, что их вообще не существует, а информация о них, постоянно публикуемая в средствах массовой информации, не более чем блеф, предназначенный для запугивания домохозяек. Но, оказывается, все не так просто и уже давно существуют ракетные системы, от которых ПРО защитить не способны, то есть не способны защитить национальную инфраструктуру от поражения ЭМИ ЯВ. Что же это за системы?

2.5 Ракетные системы малой и средней дальности – потенциальные источники ЭМИ ЯВ, против которых бессильны системы ПРО

Сегодня наблюдается тенденция снижения мощности ядерной БЧ ракет всех типов в связи с улучшением их точности. Так, например, если не очень точная Точка-У (9М79Б2) с круговым вероятным отклонением (КВО) 250 м снабжалась ядерной БЧ мощностью до 200 кт (заряд типа АА-92), то значительно более точная и новая ракета Искандер (9М723), рис. 4, с КВО до 30 м может снабжаться ядерной БЧ мощностью всего лишь 50 кт, рис. 2.3. Однако, для создания мощного и эффективного ЭМИ мощности в 50 кт не достаточно.

Широко разрекламированная, как не имеющая аналогов, российская система «Искандер» на поверку оказывается не такой уж уникальной. Очень схожими тактико-техническими данными, особенностями траектории и системы управления обладают израильские ракеты LORA (LOng Range Attack). При этом они обладают еще большей, чем «Искандер» точностью (КВО = 10 м), вдвое меньшей массой ракеты, большей массой боевой части, способной нести более мощный ядерный заряд и имеют универсальную пусковую установку, которая может монтироваться на различных транспортных средствах, включая корабли.

Рис. 2.3. Пусковые установки с тактической ракетой «Точка-У» (вверху) и оперативно-тактической «Искандер» (внизу)

Пусковая установка системы LORA, выполненная в виде контейнера с четырьмя ракетами, который по своей форме очень напоминает контейнеры российской системы «Клуб-К» (Club-K) с таким же количеством ракет 3М-14КЭ, Х-35УЭ, рис. 2.4.

Club-K — российский контейнерный комплекс ракетного оружия, размещаемый в стандартном 20- или 40-футовом морском контейнере.

Рис. 2.4. Контейнерные пусковые установки ракетных комплексов Club-K (вверху) и LORA (внизу)

Комплекс предназначен для поражения надводных и наземных целей. Комплексом могут оснащаться береговые линии, суда различных классов, железнодорожные и автомобильные платформы. Комплекс может быть применён с наземных стартовых позиций, морских, железнодорожных и автомобильных платформ. Могут применяться противокорабельные ракеты (3М-54КЭ, 3М-54КЭ1, Х-35УЭ) и ракеты для поражения наземных целей (3М-14КЭ, Х-35УЭ). Все ракеты этого комплекса крылатые, летящие на небольшой высоте 10 – 150 м и не предусмотренные для комплектации ядерными боеголовками, в то время, как израильский контейнерный комплекс LORA снабжен оперативно-тактическими ракетами, поднимающимися на высоту до 45 км и способными доставлять ядерные заряды большой мощности на расстояние до 300 км.

Почему мы так подробно рассматриваем именно эти ракетные системы? Потому, что именно такие, относительно небольшие ракеты, размещенные в стандартных морских контейнерах на кораблях, вблизи береговой линии или прямо в портах (рис. 5) и способные доставлять ядерные заряды на расстояние в сотни километров и подниматься на высоту в десятки километров, являются источниками ЭМИ, неуязвимыми для любых систем ПРО, как существующих, так и перспективных благодаря возможности скрытного приближения к цели, исключительно малого подлетного времени и изменяемой в полете траектории.

Возможность скрытно приблизить тактические ракеты с ядерными боеголовками небольшого радиуса действия близко к цели, чтобы, с одной стороны, исключить возможность их поражения средствами ПРО, а с другой - вывести из под действия ограничений международных договоров, специалисты понимали давно и попытки создать такие системы начали предприниматься сразу же с появлением относительно небольших по размеру тактических ракет с ядерными боеголовками. Так, в 1961 г. в США на вооружение воздушно-десантных частей поступила ракетная система «Little John» (MGR-3) с неуправляемыми ракетами, способными нести ядерные боеголовки. Легкие пусковые установки этой системы транспортировались вертолетами CH-47 "Chinook" как в кабине, так и на внешней подвеске.

Рис. 2.5. Контейнеры на кораблях и в портах, в которых могут находиться комплексы оперативно-тактических ракет с ядерными боеголовками, неуязвимыми для систем ПРО

В Советском Союзе быстро оценили перспективность таких систем и по Постановлению Совета министров СССР № 135-66сс от

05.02.1962 г. были начаты работы по созданию тактического ракетного комплекса «Луна-МВ» (9К53) на базе ракет 9М21Б с ядерной и 9М21Б1 с термоядерной боевой частью и пусковой установкой 9П114, представляющей собой легкую самодвижущуюся платформу с карбюраторным двигателем М-407 мощностью 45 л. с. от автомобиля «Москвич». Затем были разработаны несколько модификаций таких ракетных систем, предусматривающих транспортировку грузовыми вертолетами Ми-6 или МИ-10. Предполагалось, что вертолет может доставить ракету с пусковой установкой в тыл противника. Далее при необходимости комплекс проделает еще какой-то путь на колесах, а затем внезапно нанесет ракетный удар из точки, где враг и не мог предположить наличие ракетной установки, что фактически превращает тактический комплекс в стратегический. Работы по комплексу «Луна-МВ» достигли стадии испытаний опытных образцов. Однако встретилось довольно много трудностей, в том числе большая «парусность» вертолета с подвешенной пусковой установкой, и соответственно большой его снос ветром, а также недостаточная дальность полета нагруженных вертолетов. В результате в 1965 году работы по этому комплексу были прекращены.

Современный уровень технологий позволил вернуться к этой идее и успешно реализовать ее. Сегодня в обороте находятся сотни миллионов стандартных морских контейнеров по всему миру, рис. 2.5. И кто знает, какие из них настоящие, а какие начинены ракетами... Несмотря на то, что на сегодняшний день израильская LORA является фактически единственной полноценной контейнерной системой, способной скрытно приблизиться на контейнеровозе к побережью страны и поразить ее территорию электромагнитным импульсом, сам факт существования такой системы позволяет утверждать, что заверения представителей военно-промышленного комплекса в том, что надежно защитить от ЭМИ ЯВ могут только продвинутые системы ПРО и поэтому средства нужно вкладывать именно в эти системы, не соответствует действительности и, по-существу, являются обманом общественного мнения. Реальная ситуация такова, что армия не в состоянии обеспечить достаточно надежную защиту систем электроснабжения городов и населенных пунктов от ПЭДВ и поэтому позаботиться о такой защите заблаговременно должны сами энергетики.

2.6 Что нужно для того, чтобы реально защитить страну от «электромагнитного Армагеддона»?

Поскольку в настоящее время все необходимые базовые исследования проблемы уже давно выполнены, а их результаты и практические рекомендации опубликованы в общедоступных источниках информации [24 - 34], а также в многочисленных стандартах International Electrotechnical Commission (IEC) [34 – 41], Institute of Electrical and Electronics Engineers (IEEE) [42], военных стандартах Министерства обороны США [44 - 49], то следует прекратить финансирование огромного количества организаций, эксплуатирующих эту проблему и использующих ее в качестве источника собственного существования, а освободившиеся средства направить на осуществление вполне конкретных действий по защите электроэнергетических систем от ПЭДВ [50]. В тех странах, в которых такая разветвленная сеть организаций, занимающихся этой проблемой, как в США, еще не создана, нельзя идти по пути США и начинать создавать подобные структуры, поскольку такой путь ведет в тупик. Единственной организацией, которая должна остаться и управлять процессом, должен быть, по нашему мнению, Национальный Координационный Центр по проблеме ПЭДВ, призванный проанализировать опубликованные по этой теме работы, составить конкретный план конкретных работ со сроками и ответственными за выполнение этих сроков организациями, выдать этим организациям конкретные технические задания по защите систем электроснабжения от ПЭДВ, а затем организовать и координировать эту работу. Результатом деятельности этого Центра должны быть не отчеты и конференции (которые должны быть просто запрещены!), а реальные подстанции и электростанции, защищенные от ПЭДВ.

2.7 Классификация и особенности преднамеренных электромагнитных деструктивных воздействий

В англоязычной технической литературе преднамеренные электромагнитные деструктивные воздействия (ПЭДВ) называются “High Power Electromagnetic Threats (HPEM)” и подразделяются на два вида: высотный электромагнитный импульс ядерного взрыва (ЭМИ ЯВ) - “High-Altitude Electromagnetic Pulse (HEMP)” и пред-

намеренно излучаемые электромагнитные помехи (ПИЭМ) - “Intentional Electromagnetic Interference (IEMI)”.

ЭМИ ЯВ – очень мощный электромагнитный импульс, являющийся следствием высотного ядерного взрыва. О мощном электромагнитном импульсе, возникающем при ядерном взрыве, было известно уже давно, как об одном из поражающих факторов такого взрыва. О том, что ядерный взрыв будет обязательно сопровождаться электромагнитным излучением, следовало из теоретических исследований воздействия рентгеновского излучения американского физика-теоретика Артура Комптона, выполненных им еще 1922 году (в 1927 году за это открытие он был удостоен Нобелевской премии). В то далекое время на этот эффект не обратили особо внимания и вспомнили о нем с началом испытательных ядерных взрывов. В [2.51] об этом рассказывается так: «В конце июня 1946 года в районе атолла Бикини (Маршалловы острова) под шифром "Операция Кроссроудс" были проведены ядерные взрывы, в ходе которых исследовалось поражающее действие атомного оружия. В ходе этих испытательных взрывов было обнаружено новое физическое явление - образование мощного импульса электромагнитного излучения (ЭМИ), к которому сразу же был проявлен большой интерес. Особенно значительным оказался ЭМИ при высоких взрывах. Летом 1958 года были произведены ядерные взрывы на больших высотах. Первую серию под шифром "Хардтэк" провели над Тихим океаном вблизи острова Джонстон.

Таблица 2.1. Зона электромагнитного поражения высотного ядерного взрыва

Высота взрыва, км	Примерный диаметр зоны поражения, км
40	1424
50	1592
100	2.242
200	3.152
300	3.836
400	4.402

В ходе испытаний были взорваны два заряда мегатонного класса: "Тэк" - на высоте 77 километров и "Ориндж" - на высоте 43 километра. В 1962 году были продолжены высотные взрывы: на высоте 450 км под шифром "Старфиш" был произведен взрыв боеголовки мощностью 1,4 мегатонны. Советский Союз также в течение 1961-1962 гг. провел серию испытаний, в ходе которых исследовалось воздействие высотных взрывов (180-300 км) на функционирование аппаратуры систем ПРО. При проведении этих испытаний были зафиксированы мощные электромагнитные импульсы, которые обладали большим поражающим действием на электронную аппаратуру, линии связи и электроснабжения, радио- и радиолокационные станции на больших расстояниях.

Зависимость зоны эффективного поражения электронной аппаратуры от высоты подрыва заряда мощностью 10Мт приведены в таблице 2.1.

В соответствии с классификацией Международной электротехнической комиссии (МЭК) Выделяют три компонента ЭМИ ЯВ: Е1, Е2 и Е3, рис. 2.6.

Е1 – самый «быстрый» и самый «короткий» компонент ЭМИ ЯВ, обусловленный мощным потоком Комптоновских электронов высокой энергии (являющихся продуктом взаимодействия γ-квантов мгновенного излучения ядерного взрыва с атомами газов воздуха) движущихся в магнитном поле Земли с околосветовой скоростью.

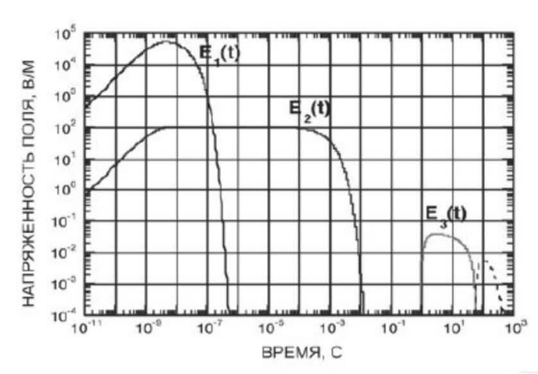


Рис. 2.6. Параметры компонентов высотного ядерного взрыва (IEC 61000-2-9)

Это взаимодействие очень быстро движущихся отрицательно заряженных электронов с магнитным полем производит импульс электромагнитной энергии, сконцентрированной магнитным полем Земли и направленной с высоты на Землю. Амплитуда импульса обычно нарастает до своего пикового значения в течение 5 наносекунд и спадает вдвое в течение 200 наносекунд. По определению МЭК, полная продолжительность импульса Е1 может составлять около одной микросекунды (1000 наносекунд). Компонент Е1 обусловлен самым интенсивным электромагнитным полем, вызывающим очень высокие напряжения в электрических цепях, он создает вблизи уровня земли на умеренно высоких широтах импульсные напряжения до 50 кВ/м при плотности мощности 6,6 МВт на квадратный метр. Компонентом Е1обусловлено большинство повреждений электронного оборудования, связанных с воздействием перенапряжений и электрическим пробоем *p-n*-переходов полупроводниковых элементов и изоляции. Обычные разрядники, эффективные для защиты от атмосферных перенапряжений, не всегда успевают сработать и защитить оборудование при воздействии компонента Е1, а рассеиваемая ими мощность далеко не всегда достаточна для поглощения энергии компонента Е1 импульса, в результате чего обычные разрядники могут просто разрушиться.

Е2 – это «промежуточный» по скорости нарастания и длительности компонент ЭМИ который, по определению МЭК, длится примерно от 100 мкс до 1 мс. Компонент Е2 имеет много общего с электромагнитными импульсами, атмосферного происхождения (близкой молнией). Напряженность поля может достигать 100 кВ/м. Из-за сходства параметров компонента Е2 с молнией и хорошо отработанными технологиями защиты от молнии, считается, что защита от компонента Е2 не представляет проблемы. Однако, при совместном воздействии компонентов Е1 и Е2 появляется проблема другого рода, когда под действием компонента Е1 разрушаются защитные элементы, после чего компонент Е2 беспрепятственно проникает в аппаратуру.

Компонент **Е3** очень отличается от двух других основных компонентов ЭМИ. Это очень «медленный» импульс, длящийся десятки-сотни секунд, что обусловлено смещением и последующим восстановлением магнитного поля Земли. Компонент Е3 имеет сходство с геомагнитной бурей вызванной очень интенсивной солнеч-

ной вспышкой. Геомагнитные индуцированные токи – это токи, протекающие в земле, вызванные геомагнитными возмущениями в магнитосфере Земли. Эти токи наводятся и в протяженных металлических предметах, находящихся в земле, таких как трубопроводы, рельсы железных дорог, кабели. Напряженность индуцированного поля может доходить до 1В/км. Сильные возмущения в магнитосфере земли возникают во время солнечных бурь, сопровождающихся выбросом огромного количества ионизированной плазмы в направлении Земли, рис. 2.7. В ионосфере Земли, расположенной в нескольких сотнях километров над поверхностью Земли, под действием магнитного поля Земли и её вращения вокруг своей оси всегда протекают электрические токи. Они поддерживаются за счёт постоянного образования большого количества заряженных частиц — ионов и свободных электронов из расщепляемых солнечной радиацией молекул атмосферных газов. Эти электрические токи оказывают существенное влияние на формирование магнитного поля Земли. Во время солнечных бурь особо мощные потоки протонов и электронов солнечной плазмы резко увеличивают электрические токи, протекающие в ионосфере.

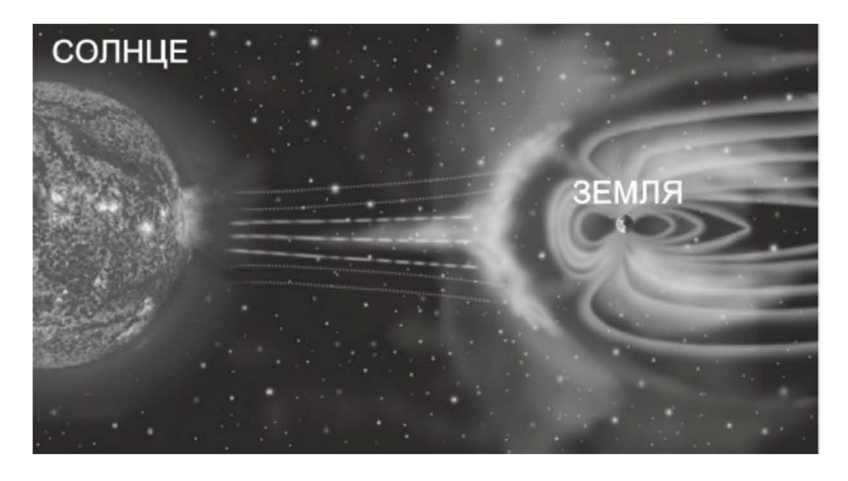


Рис. 2.7. Искажение магнитного поля Земли под воздействием выбросов Солнечной плазмы

Резкие изменения этих токов приводят не только к резким изменениям магнитного поля Земли, но и к возникновению геомагнитных индуцированных токов и наведению больших токов в протяженных линиях электропередач. Эти наведенные токи замыкаются через заземленные нейтрали силовых трансформаторов, рис. 2.8. Поскольку эти токи имеют очень низкую частоту, то их протекание через обмотки трансформаторов приводит к насыщению магнитопроводов трансформаторов и к резкому снижению их импеданса. Как известно, постоянная составляющая в токе силового трансформатора появляется также в момент его включения, поэтому реле защиты силовых трансформаторов обычно отстроены от постоянной составляющей в токе и не реагируют на нее. Кроме того, постоянный ток (или ток очень низкой частоты) практически не передается через трансформаторы тока. Таким образом, обычная релейная защита не будет реагировать на индуцированные токи, насыщающие трансформатор и он просто сгорит. В истории известны случаи сгорания силовых трансформаторов под действием геомагнитных индуцированных токов во время солнечных бурь. Так, в 1989 г. скромный по масштабам солнечный шторм привел к повреждению силовых трансформаторов сверхвысокого напряжения и на 9 часов погрузил во тьму канадскую провинцию Квебек.

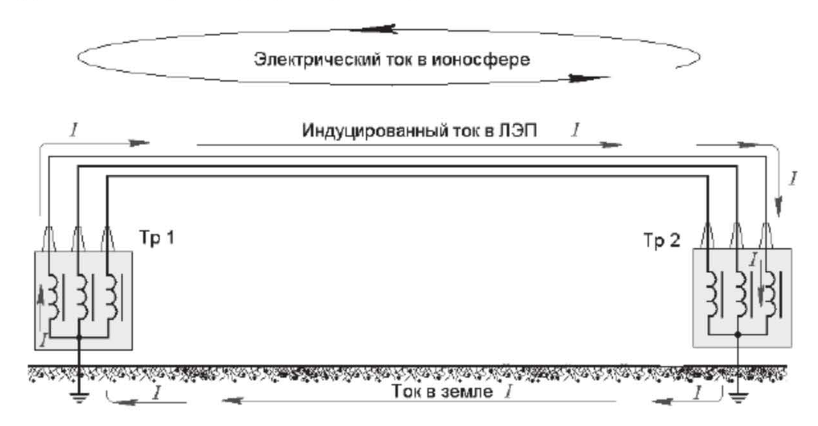


Рис. 2.8. Схема наведения токов в ЛЭП и земле электрическими токами ионосферы

На АЭС Salem в американском штате Нью Джерси в это же время вышел из строя мощный силовой трансформатор сверхвысокого напряжения. 29 апреля 1994 г. вскоре после начала сильной геомагнитной бури на АЭС Maine Yankee полностью был выведен из строя мощный трансформатор сверхвысокого напряжения. 24 марта 1940 г. из-за сильнейшей геомагнитной бури было временно нарушено электроснабжение в некоторых регионах штатов Новой Англии, Нью-Йорка, Пенсильвании, Миннесоты, Квебека и Онтарио, выведено из строя 80 % всех магистральных телефонных сетей в Миннеаполисе [2.52]. Необычайно сильная солнечная буря прогнозировалась учеными NASA в 2012 (по некоторым прогнозам в 2013 г.). По прогнозам [2.52] и в другие периоды в ближайшие годы возможны сильные магнитные бури при которых по всему миру ожидаются сбои в энергосистемах. Они займут от нескольких часов до нескольких месяцев (в связи с отсутствием во многих энергосистемах резервных силовых трансформаторов). Это грозит настоящим коллапсом для современного человечества, слишком зависимого от современных технологий и уязвимого к катастрофам такого рода.

Аналогичные, по своей физической природе, воздействия на силовые трансформаторы оказывает и компонент Е3 высотного ядерного взрыва [2.52]. Особенностью силовых трансформаторов является то, что в случае выхода из строя их невозможно быстро заменить, в отличие от электронных приборов, которые также подвержены повреждениям при таких воздействиях.

В связи с выше изложенным, становится понятной актуальность решения проблемы защиты силовых трансформаторов от повреждения при воздействии индуцированных геомагнитных токов низкой частоты.

С 80-х годов прошлого столетия в ряде стран мира усиленно работают над созданием так называемого «Супер-ЭМИ» ядерного заряда с усиленным выходом электромагнитного излучения. Работы ведутся в основном в двух направлениях: за счет создания вокруг заряда оболочки из вещества, испускающего γ–излучение высокой энергии при облучении его нейтронами ядерного взрыва, а также за счет фокусировки γ –излучения. По расчетам специалистов, с помощью Супер-ЭМИ можно будет создать напряженность поля у поверхности Земли порядка сотен и даже тысяч киловольт на метр.

Причем, военные и не скрывают, что главными целями такого ЭМИ оружия в будущих конфликтах будут системы государственного и военного управления, национальная инфраструктура, включающая системы электро- и водоснабжения, связи.

В июне 1950 года в составе 12 Главного управления Министерства обороны СССР в г. Сергиев Посад-7 (поселок «Ферма») даже был создан Центральный физико-технический институт МО РФ, получивший номер В/ч 51105 (сегодня это ФГУ "12 ЦНИИ МО РФ"), возглавлял который академик Владимир Михайлович Лоборев (с 2002 г. начальник института - контр-адмирал, д.т.н, профессор, Перцев Сергей Федорович).

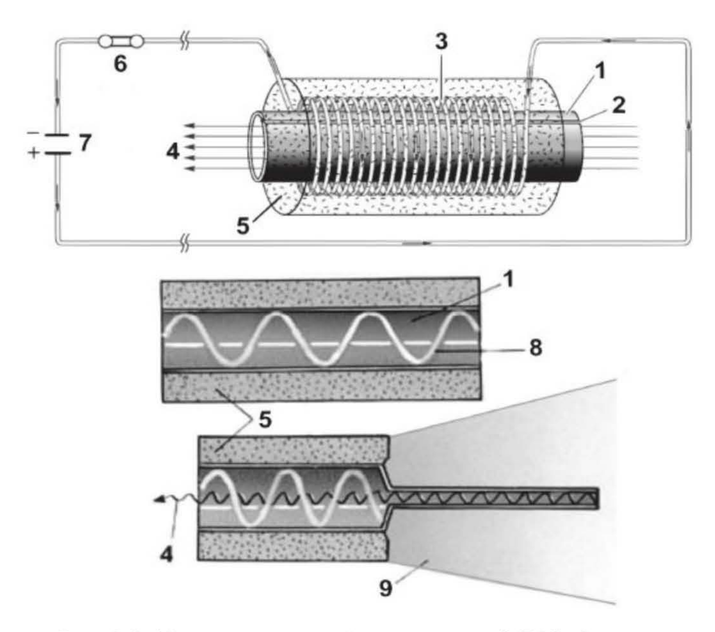


Рис.2.9. Ударно-волновой излучатель (УВИ). 1 - электромагнитный резонатор; 2 – разрез; 3 – катушка, обтекаемая током; 4 - направленное электромагнитное излучение; 5 – взрывчатое вещество; 6 – коммутатор; 7 – накопитель энергии (конденсатор); 8 – стоячая волна; 9- разлетающиеся продукты взрыва

Основной задачей этого института были исследования поражающих факторов ядерного взрыва, в основном, электромагнитного импульса, а также лазерного, пучкового, СВЧ оружия, рентгеновского излучения и т.п. Среди экспериментальных установок института известны сверхмощные генераторы импульсов высокого напряжения ГИН-10; имитаторы электромагнитного импульса ядерного взрыва ИЭМИ-Б и ИЭМИ-БМ; комплексы «Артерит» и «Зенит» для испытаний техники на воздействие электромагнитного импульса, импульсный ядерный реактор «БАРС» и др.

Мощный ЭМИ можно создать не только в результате ядерного взрыва. Современные достижения в области неядерных генераторов ЭМИ позволяют сделать их достаточно компактными для использования с обычными и высокоточными средствами доставки. Поэтому вопросы защищенности от воздействия ЭМИ будут оставаться в центре внимания специалистов при любом исходе переговоров о ядерном разоружении.

ПИЭМ – второй тип преднамеренных деструктивных электромагнитных воздействий, не связанный с ядерным взрывом.

Первые теоретические идеи о возможности создания неядерных ударно-волновых излучателей сверхмощных электромагнитных импульсов (УВИ) были высказаны в 1951 году академиком Андреем Сахаровым при работе над ядерным боезарядом в Арзамасе-16 (ныне Всероссийский научно-исследовательский институт экспериментальной физики – ВНИИЭФ).

Первые экспериментальные работы по получению сверхмощных импульсных магнитных полей путем их взрывного сжатия были начаты в этом институте Робертом Лобаревым, которым в 1952 году удалось получить импульсные магнитные поля в полтора миллиона Гаусс (для сравнения, магнитное поле Земли составляет около 0,3 Гаусс на экваторе и 0.7 Гаусс в полярных районах). В дальнейшем эти работы были продолжены Александром Павловским и Владимиром Чернышевым из того же института. Коллективу под руководством А. Павловского удалось построить взрывной генератор, рис. 2.9, с импульсным током в 200 миллионов ампер, генерировавшим магнитное поле в 10 миллионов Гаусс.

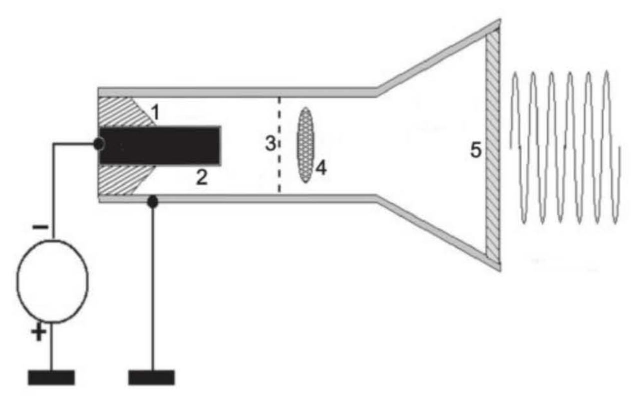
Ударно-волновой излучатель сверхмощных электромагнитных импульсов представлял собой кольцо из взрывчатого вещества, окружающего медную катушку. Набор подрываемых синхронно

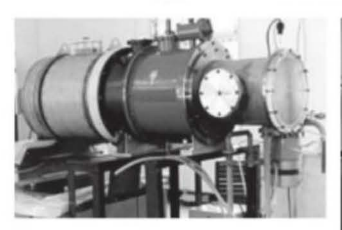
детонаторов инициировал детонацию, направленную к оси. В момент, синхронизованный с подрывом, происходит разряд мощного конденсатора, ток которого формирует магнитное поле внутри катушки. Ударная волна огромным давлением (около миллиона атмосфер) сминает и «закорачивает» витки катушки, превращая ее в трубку и замыкая это поле внутри нее. Контур с током сжимается со скоростью в несколько километров в секунду, в зависимости от типа взрывчатки. Как известно из физики, интенсивность магнитного потока, создаваемая контуром в этом случае, пропорциональна скорости изменения индуктивности по времени. Поскольку размер катушки меняется с огромной скоростью при схлопывании контура, то соответственно и амплитуда магнитного потока получается также огромной (десятки миллионов ампер). В этот момент с помощью пиропатрона разрушают один из торцов резонатора, а ударная волна, сойдясь в точку и отразившись, устремится обратно, скачком изменив поле. При этом стоячая волна превращается в бегущую, развивая при этом огромную импульсную мощность, что и приведет к генерации импульсного потока радиочастотного электромагнитного излучения. За доли наносекунды поле меняется, но не по закону синуса с периодом, равным времени сжатия-разрежения, а более резко, и это значит, что в функции, описывающей его изменение, присутствуют многие частоты. Поэтому ударно-волновой источник является сверхширокополостным и излучает в диапазоне от сотен мегагерц до сотен гигагерц при продолжительности этого импульса десятки-сотни микросекунд.

Практически одновременно и независимо с ними в Лосс-Аламосской Национальной Лаборатории США такие же поля были получены группой, возглавляемой Максом Фоулером (Max Fowler). Оба ученых впервые встретились в Новосибирске в 1982 году на Международной конференции по сверхмощным магнитным полям, а в 1989 г. группу советских ученых под руководством А. Павловского уже встречали в Лосс-Аламосской лаборатории.

Практически с самого начала этих работ не только ученым в США и СССР, но и политикам стало понятно, что такого рода источники сверхмощных электромагнитных импульсов могут стать основой для создания нового вида оружия. Свидетельством этому стали выступления Н. С. Хрущева в 60-х годах с его упоминаниями

некоего «фантастического оружия», разрабатываемого советскими учеными.





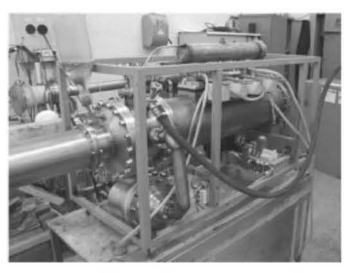
Виркаторы с индуктивным (слева) и емкостным (справа) накопителями энергии

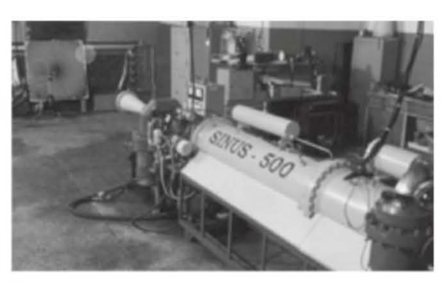
1.	Напряжение	400 кВ
2.	Ток в виркаторе	12 кА
3.	Длительность импульса напряжения	300 нс
4.	Мощность излучения	350 МВт
5.	Длительность импульса излучения	200 нс.
6.	Частота излучения	3.1 ГГц

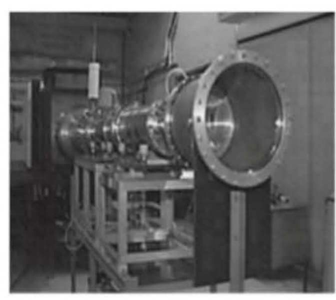
1.	Напряжение	600 кВ
2.	Ток в виркаторе	18 кА
3.	Длительность импульса напряжения	100 нс
4.	Мощность излучения	500 МВт
5.	Длительность импульса излучения	80 нс.
6.	Частота излучения	3.1 ГГц.

Рис. 2.10. Мощные виркаторы, разработанные в Томском политехническом институте. 1 – изолятор; 2 – металлический катод; 3 – сеточный анод; 4 – виртуальный катод; 5 – диэлектрическое окно

Об УВИ, как о самостоятельном устройстве для создания сверхмощных электромагнитных импульсов, в качестве оружия, впервые было официально заявлено начальником Лаборатории боеприпасов специального назначения ЦНИИ Химии и Механики докт.техн.наук А. Б. Прищепенко после успешных испытаний 2 марта 1983 г. на полигоне Красноармейского научно-исследовательского института «Геодезия», Моск. обл. (ныне ФКП НИИ «Геодезия»).







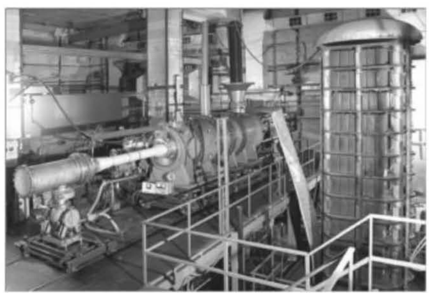


Рис. 2.11. Релятивистские микроволновые генераторы большой мощности на базе гиротронов, виркаторов и ламп обратной волны, разработанные в различных Российских НИИ

Позднее, членом-корреспондентом Академии военных наук, докт.техн.наук А. Б. Прищепенко были сформулированы общие принципы боевого применения электромагнитных боеприпасов.

Сегодня интенсивные исследования в области ПИЭМ ведутся в нескольких направлениях и неядерные ударно-волновые излучатели

(УВИ) уже не являются единственным видом неядерного электромагнитного оружия.

Существует широкий набор микроволновых устройств высокой мощности. Релятивистские клистроны и магнетроны, рефлекс-триоды, лампы обратной волны (ЛОВ), гиротроны, осцилляторы с виртуальным катодом - виркаторы (Virtual Cathode Oscillator - Vircator) и другие, рис. 2.11.

Виркаторы способны произвести очень мощные одиночные импульсы энергии, конструктивно простые, небольшие по размерам, прочные и способные работать в относительно широкой полосе частот микроволнового диапазона. Фундаментальная идея, лежащая в основе виркатора, заключается в ускорении мощного потока электронов сетчатым анодом. Этот мощный поток электронов изначально вырывается из катода (металлического цилиндрического стержня диаметром в несколько сантиметров, рис. 2.10) под действием импульса высокого напряжения (сотни киловольт), придающего эмиссии электронов взрывной характер. Значительное число электронов проходит через сетчатый анод, формируя облако пространственного заряда за анодом. При определенных условиях, эта область пространственного заряда будет осциллировать в области анода.

Образованное на частоте колебаний электронного облака СВЧ-поле излучается в пространство через диэлектрическое окно. Стартовые токи в виркаторах, при которых возникает генерация, составляют 1–10 кА. Виркаторы, рис. 2.11, наиболее приемлемы для генерации импульсов наносекундной длительности в длинноволновой части сантиметрового диапазона. Экспериментально на них получены мощности от 170 кВт до 40 ГВт в сантиметровом и дециметровом диапазонах. По опубликованным данным, экспериментальная установка, развивающая импульсную мощность около 1 ГВт (265 кВ, 3,5 кА) способна поражать электронную аппаратуру на расстоянии 800 - 1000 м.

Даже такие хорошо известные устройства, как высоковольтные импульсные генераторы Маркса, рис. 2.12, содержащие набор высоковольтных конденсаторов и разрядников (80 одинаковых блоков), могут использоваться как мощные источники микроволнового излучения. В этом устройстве все конденсаторы сначала заряжаются параллельно от высоковольтного источника, а в момент син-

хронного пробоя управляемых разрядников все конденсаторы оказываются соединенными последовательно.

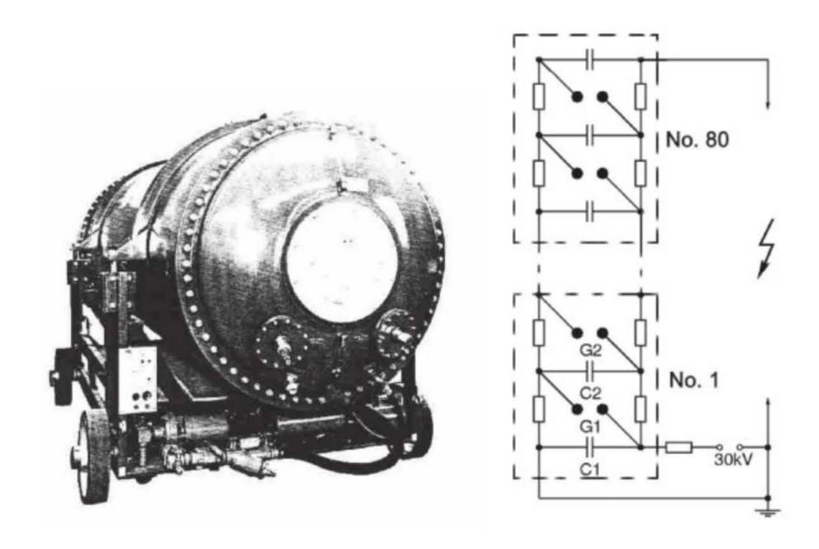


Рис. 2.12. Американский FEBETRON-2020 на базе генератора Маркса и его упрощенная схема

В передвижном генераторе FEBETRON-2020, рис. 2.12, генерируются импульсы тока в 6 кА при напряжении 2.3 МВ, в результате чего излучаются мощные электромагнитные импульсы. На основе схемы Маркса американская компания Applied Physical Electronics разработала целую серию мощных ультра компактных генераторов на напряжения до 1 МВ с излучаемой пиковой мощностью до 6 ГВт, рис. 2.13. Снабженные параболической антенной, рис. 2.14, эти устройства способны излучать разрушительную для электроники направленную энергию СВЧ огромной мощности.

Еще одним направлением развития ПИЭМ является так называемое «пучковое оружие» (beam weapon). Это оружие основано на использовании узконаправленных пучков заряженных или

нейтральных частиц, генерируемых с помощью различных типов ускорителей как наземного, так и космического базирования.

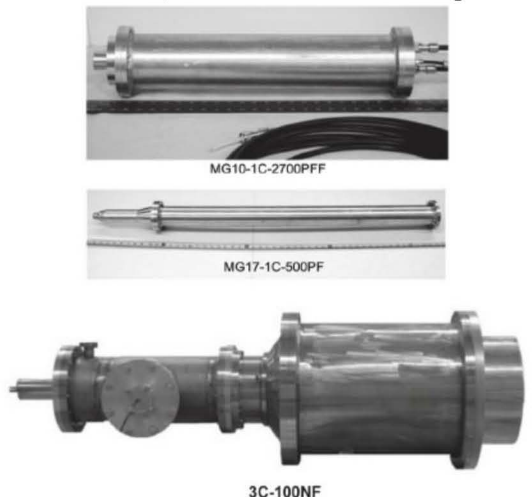


Рис. 2.13. Компактные генераторы Маркса большой мощности 300 кВ, 1 ГВт (MG10-1C-2700PFF), 510 кВ, 400 МВт (MG17-1C-500PF), 600 кВ, 6 ГВт (MG30-3C-100NF)

Рис. 2.14. Мощный генератор направленного микроволнового излучения на основе компактного генератора Маркса и параболической антенны

Работы по созданию пучкового оружия получили наибольший размах вскоре после провозглашения в 1983 г. президентом США Рональдом Рейганом программы Стратегической Оборонной Инициативы (СОИ).

Центром научных исследований в этой области стала Лос-Аламосская национальная лаборатория, а также Ливерморская национальная лаборатория, а в России – ФГУ «12 ЦНИИ МО РФ». По заявлению некоторых ученых, там предпринимались успешные попытки получить поток высокоэнергетических электронов, по мощности превосходящий в сотни раз получаемый в исследовательских ускорителях.

Рис. 2.15. Компактные мощные сверхширокополостные источники излучения мощностью до 1 ГВт, разработанные в Томском НИИ Сильноточной Электроники СО РАН

В этой же лаборатории в рамках программы «Антигона» было экспериментально установлено, что электронный пучок почти идеально, без рассеяния, распространяется по ионизированному каналу, предварительно созданному лучом лазера в атмосфере.

Большую опасность представляют собой мощные компактные источники излучения, которые могут быть смонтированы в закрытом фургоне грузовика и даже в микроавтобусе. Так, в Томском НИИ Сильноточной Электроники СО АН СССР, созданным в 1977 г. специально для исследований методов генерации сверхмощных (гига– и терраваттных) электрических импульсов и возглавляемом академиком Г. А. Месяцем разработаны достаточно компактные генераторы мощных (100-1000 МВт) линейно поляризованных однонаправленных волновых пучков сверхширокополосного электромагнитного излучения с наносекундной и субнаносекундной дли-

тельностью импульса специально для воздействия на электронную аппаратуру, рис. 2.15.

Рис. 2.16. Компактный источник мощного направленного ультракоротковолнового (95 ГГц) излучения, разработанный американской Sandia National Laboratories, с использованием технологий компании Raytheon (вверху), а также мощные источники направленного излучения, смонтированные на шасси джипа Hummer и на шасси БТР Stryker. Еще более мощный комплекс планируется установить на борту самолета АС-130

Причем, такие источники можно сегодня совершенно свободно приобрести непосредственно в Институте за совсем не «космическую» цену в 40-60 тысяч долларов и установить в микроавтобусе или в небольшом фургоне.

Все координаты для заказа этой аппаратуры приведены на официальном сайте Института.

Аналогичные переносные и передвижные источники разрабатываются и производятся в США, рис. 2.16.

По сообщениям, опубликованным в печати, в октябре 2012 г. компания «Боинг» провела на полигоне «Юта» в условиях, приближенных к боевым, испытаний ракеты, созданной в рамках программы CHAMP (проект усовершенствованной ракеты с мощным микроволновым излучателем для борьбы с радиоэлектронными средствами). В ходе испытаний ракета CHAMP (Counter-electronics High-powered Microwave Advanced Missile Project), выполнявшая полет по заложенной программе, генерировала мощные энергетические импульсы, эффективно выводя из строя электронные подсистемы и уничтожая данные без нанесения физических разрушений. Ракета CHAMP продемонстрировала способность осуществлять выборочные и точно рассчитанные атаки на несколько целей в течение одного вылета, используя мощный микроволновой излучатель HPM (High-Powered Microwave). Наблюдение за полетом осуществлялось с авиабазы «Хилл».

CHAMP должен стать нелетальной альтернативой системам вооружения кинетического действия и традиционным средствам поражения взрывного действия при нанесении ударов по объектам противника, оснащенным радиоэлектронной аппаратурой. Ракета позволяет вывести из строя объект, повредив его электронику и нанеся минимальный побочный физический ущерб району размещения.

По оценке руководителя программы в «Боинг Фантом Уоркс» Кейта Коулмана, разработанная технология знаменует новую эру в современной войне. В ближайшем будущем она может использоваться для вывода из строя электронного оборудования и информационных систем противника без применения авиации и сухопутных сил. По заявлению «Боинга», проект является адаптацией разработанной лабораторией ВВС США технологии направленной энергии на платформу созданной компанией ракеты и станет базой для создания нового семейства высокоэффективных систем вооружения нелетального действия.

Выступая в качестве главного подрядчика, «Боинг» изготовляет воздушную платформу и осуществляет окончательную интеграцию всех систем. Компания «Рейтеон» поставила источник микроволнового излучения HPM, а национальная лаборатория «Сандия» обес-

печивает по отдельному контракту с Научно-исследовательской лабораторией ВВС США поставку системы питания.

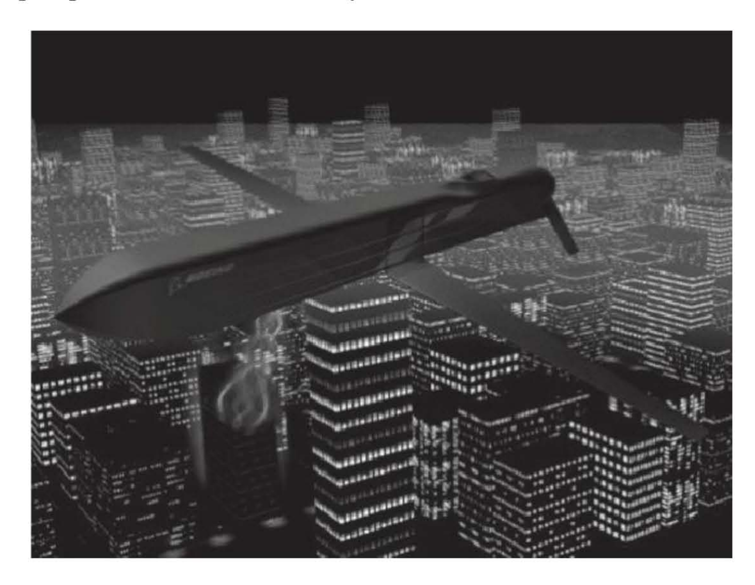


Рис. 2.17. Реклама крылатой ракеты с электромагнитной боевой частью CHAMP фирмы Боинг

В рекламном ролике фирмы «Боинг», посвященной этой программе показана крылатая ракета, рис. 2.17, пролетающая над городом и «гасящая» его огни. В частности, мелькает главный диспетчерский щит электростанции, на котором погасают все сигналы при пролете ракеты.

В связи с высокой технологичностью, электромагнитным оружием в мире занимаются очень ограниченное количество компаний. Мировыми лидерами являются американские Northrop Grumman, Lockheed Martin, Raytheon, ITT и британская BAe Systems. В России ведущий отечественный разработчик и изготовитель средств ведения радиоэлектронной войны – ОАО «Концерн Радиоэлектронные технологии». Образованный в 2009 году холдинг объединил под своей эгидой 18 предприятий – научно-исследовательские институты, конструкторские бюро и серийные заводы, специализирующие-

ся на создании средств ведения радиоэлектронной войны авиационного, морского и наземного базирования. В рамках реализации Государственной программы вооружения на период 2011–2020 годов (ГПВ-2020) концерн планомерно наращивает свое присутствие на рынке средств ведения радиоэлектронной войны.

Рис. 2.18. Мобильная станция радиэлектронного подавления 1Л269 "Красуха-2"

За последнее время успешно прошли государственные испытания и поставлены на серийное производство комплексы «Москва-1», «Красуха-2», «Красуха-4», «Ртуть-БМ» и ряд других, рис. 2.18, разработанные ВНИИ «Градиент», входящем в концерн. Мобильная микроволновая система «Ранец-Е» (разработчик - Московский радиотехнический институт) с импульсной излучаемой мощность 500 МВт обеспечивает гарантированное поражение электроники на дальностях до 12-14 километров, а серьезные нарушения в ее работе наблюдаются на расстоянии до 40 км, рис. 2.19. Фактически – это мощная микроволновая пушка, специально предназначенная для поражения электронного оборудования. Ее недостатком является большой вес (свыше 5 тонн) и самое главное - необходимость паузы длительностью около 20 минут между каждым «выстрелом».

Недавно в печати появились сведения о создании в России аналога американской CHAMP: новой ракетной системы «Алабуга»

(ранее аналогичные ракетные системы уже выпускались в России) с особо мощным импульсным излучателем.

Рис. 2.19. Мобильная система сверхмощного СВЧ излучения большой дальности «Ранец-Е»

Боевой блок этой ракеты, будучи подорванным на высоте около 200 м способен уничтожить всю электронику в радиусе 3.5 км. Принципиальным отличием «Алабуги» от американской CHAMP является принцип действия: в «Алабуге» используется одноразовый ударно-волновой излучатель, тогда как в американской системе – виркатор, способный работать в непрерывном режиме.

В 80-х годах прошлого века известным советским ученым проф. Греховым И. В. из Физико-технического института имени А.Ф.Иоффе (С.-Петербург) были выполнены теоретические и экспериментальные работы по формированию высоковольтных наносекундных перепадов напряжения на обычных высоковольтных полупроводниковых диодах [2.53 – 2.55]. Явление возникновения перенапряжений в момент переключения силовых полупроводниковых диодов с прямого направления на обратное хорошо известно в технике и с ним борются различными способами, поскольку такие перенапряжения снижают надежность работы и самих диодов, и других элементов электронных схем. В работах, начатых под руководством И. В. Грехова, этот эффект попытались наоборот усилить и использовать для генерации мощных наносекундных импульсов.

путем использования полупроводниковых высоковольтных диодов в качестве прерывателей тока в мощных импульсных системах с индуктивным накопителем энергии.

В дальнейшем эти работы были продолжены в Уральском отделении Института электрофизики РАН (г. Екатеринбург). Эксперименты, проведенные в 1991-92 г. Любутиным С.К., Рукиным С.Н. и Тимошенковым С.П. на обычных высоковольтных выпрямительных полупроводниковых диодах показали, что при определенном сочетании плотности прямого и обратного тока и времени его протекания через полупроводниковую структуру диода время спада обратного тока уменьшается до десятков-единиц наносекунд. Характерные значения плотности тока при этом составляют десятки килоампер на квадратный сантиметр, а время протекания тока лежит в диапазоне сотен наносекунд.

Рис. 2.20. SOS-диод типа SOS-180-12 (180 кВ, 12 кА)

Этот новый эффект наносекундного обрыва сверхплотных токов в полупроводниках позже получил название SOS-эффекта (от Semiconductor Opening Switch) [2.56].

В дальнейшем была разработана специальная полупроводниковая структура со сверхжестким режимом восстановления, на основе которой удалось создать высоковольтные полупроводниковые прерыватели нового класса – SOS-диоды, имеющие рабочее напряжение в сотни киловольт, ток коммутации – в десятки килоампер,

время коммутации – единицы наносекунд и частоту коммутации – килогерцы.

Типовая конструкция SOS-диода – это последовательная сборка элементарных диодов, взаимно стянутых диэлектрическими шпильками между двумя пластинами-электродами, рис. 2.20 [2.57].

На основе SOS-диодов в Уральском отделении Института электрофизики РАН разработана серия многоразовых мобильных компактных SOS-генераторов электромагнитных импульсов наносекундного диапазона с рекордными для полупроводниковых коммутаторов параметрами, рис. 2.21.

Рис. 2.21. SOS-генераторы некоторых типов, разработанные в УО Института электрофизики РАН

По сведениям, представленным на официальном сайте УО Института электрофизики РАН, эти генераторы основаны на использовании твердотельной системы коммутации энергии, в которой применяются тиристоры или транзисторы во входном устройстве, магнитные ключи в промежуточном устройстве сжатия энергии, и полупроводниковый прерыватель тока на SOS-диодах в оконечном усилителе мощности. Разработанные генераторы имеют следующий

диапазон выходных параметров: амплитуда импульса напряжения 50 кВ – 1 МВ, импульсный ток 1 – 10 кА, пиковая мощность 100 МВт – 4 ГВт, длительность импульса 3 – 60 нс, частота следования импульсов от сотен Гц до единиц кГц.

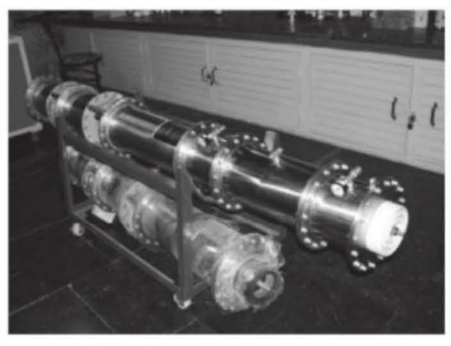


Рис. 2.22. Направленные микроволновые генераторы самодельного изготовления, описания которых приведены в популярных технических журналах

В некоторых странах (США, Израиль и др.) ведутся разработки компактных электромагнитных ружей относительно небольшой мощности, способных, однако, поражать электронику на расстояниях до 100 м. Интерес к устройствам такого рода проявляют не только военные, но и полицейские. Современный автомобиль, напичканный электроникой, представляет собой такой же объект поражения, как и любая другая современная система. Американская компания Eureka Aerospace разработала и запустила в производство электромагнитный «остановитель» движущегося автомобилей (EMP car-stopper). Действие такого оружия основано на повреждении микропроцессора, системы зажигания, впрыска топлива и др. электронных систем современного автомобиля. Что будет, когда такое оружие попадет в руки террористов (рано или поздно, но это обязательно произойдет) и они применят его против объектов электроэнергетики? Впрочем, им даже не нужно особенно искать такое оружие. Описаниями самодельных систем такого рода пестрят страницы многих популярных технических журналов, рис. 2.22.

Такие самодельные источники направленного сверхвысокочастотного излучения достаточно большой мощности, смонтированные в закрытом кузове небольшого грузовичка или даже пикапа на базе легковушки с пластмассовым кунгом, рис. 2.23, могут представлять собой серьезную опасность для объектов электроэнергетики (и не только). Можно легко представить, как такая легковушка с включенным генератором проезжает мимо современной подстанции с множеством работающих микропроцессорных устройств защиты и управления, но трудно предсказать, что при этом произойдет в энергосистеме. А ведь такая «легковушка» может в течение нескольких часов «погасить» сразу несколько подстанций. А если таких «легковушек» будет несколько?

Да и промышленность вносит свою лепту в «общее дело» выпуская подобные устройства, смонтированные в небольшом чемодане, рис. 2.24, как будто специально предназначенные для террористов. Недаром о нем упоминалось даже в докладе одного из конгрессменов США.

И как тут не вспомнить пророческое изречение Уинстона Черчилля, сделанное им много лет назад: «Каменный век может вернуться на сияющих крыльях науки».

Рис. 2.23. Источник направленного сверхвысокочастотного излучения смонтированный в пикапе на базе легковушки с пластмассовым кунгом

Рис. 2.24. Походный «разрушитель электроники» под названием «2100 Series Suitcase» на основе генератора Маркса, производимый компанией Applied Physical Electronics

2.8 Воздействие ПЭДВ на микропроцессорные устройства релейной защиты

Путями проникновения электромагнитных излучений в электронную аппаратуру являются, прежде всего, различные антенные устройства и кабельные вводы, системы электропитания, а также токи, наводимые в обшивке, и излучения, проникающие через окна и двери, выполненные из неэлектропроводных материалов, вентиляционные каналы. Токи, наводимые ЭМИ в наземных и заглубленных кабелях электропитания протяженностью в сотни и тысячи километров, могут достигать тысяч ампер, а напряжение в разомкнутых цепях таких кабелей миллион вольт. В антенных вводах, длина которых не превышает десятков метров, наводимые ЭМИ токи могут иметь силу в несколько сотен ампер. ЭМИ, проникающий непосредственно через элементы сооружений из диэлектрических материалов (неэкранированные стены, окна, двери и т.п.), может наводить во внутренней электропроводке токи силой в десятки ампер. Особую опасность представляют собой длинные воздушные линии электропередач, абсорбирующие излучение с больших площадей и доставляющих его прямо к месту назначения – на входы высокочувствительной электронной аппаратуры. Наличие на этом пути трансформаторов (измерительных и силовых) практически не сказывается на этом процессе из-за значительной внутренней емкости между первичной и вторичной обмотками. А поскольку слаботочные цепи и радиоэлектронные приборы нормально действуют при напряжениях в несколько вольт и токах силой до нескольких десятков миллиампер, то для их надежной защиты от ЭМИ требуется обеспечить снижение величины токов и напряжений на их входах на несколько порядков. Помимо собственно МУРЗ, повышенной чувствительностью к ЭМИ обладают, как это ни странно, оптические системы передачи данных, широко используемые в релейной защите. Вернее, контроллеры, преобразующие электрические сигналы в оптические на одном конце волоконно-оптической линии связи (ВОЛС) и восстанавливающие их из оптических на втором конце ВОЛС. Например, испытания на соответствие стандартам IEC по электромагнитной совместимости мультиплексора типа FOCUS [2.58], показал, что они не всегда выдерживают без сбоев и повреждений даже стандартные воздействия. Система SCADA с ее

большим количеством микропроцессорных датчиков и измерительных преобразователей, объединенных в компьютерную сеть – еще один объект воздействия даже ослабленных ЭМИ.

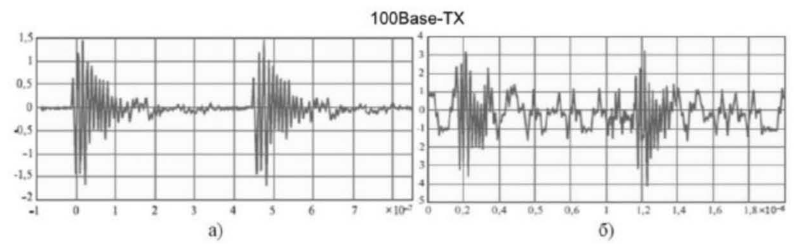


Рис. 2.25. Типовая осциллограмма наведенных импульсных помех ЭМИ в линии связи Ethernet. а) без передачи данных; б) при передаче данных (спецификация 100Base-TX) [2.59]

Если к возможности использования мощного высотного ядерного взрыва для электромагнитного поражения национальной энергосистемы еще можно относиться как гипотетической, то поражение террористическими структурами отдельных локальных энергосистем с помощью одновременного воздействия на несколько наиболее важных узлов энергосистемы с помощью неядерных источников ЭМИ – вполне возможно в любой момент.

Наиболее уязвимы для воздействия преднамеренных электромагнитных воздействий оказываются системы передачи данных, использующие протоколы с широкой полосой частот. К ним относятся ATM 155, Fast Ethernet, Gigabit Ethernet и другие, рис. 2.25. Последнее объясняется незначительной разницей мощности полезного сигнала и помех в верхней области спектра. Переход от коаксиального кабеля к простой витой паре с целью удешевления кабеля (что наблюдается сегодня повсеместно) ведет к еще большей уязвимости системы. А ведь Ethernet на базе витой пары уже сегодня начинает использоваться в релейной защите и, в соответствии со стратегией Smart Grid, его использование для управления всеми объектами в электроэнергетике будет только расширяться.

Дискретные электронные элементы имеют гораздо более высокую устойчивость к перенапряжениям и другим неблагоприятным воздействиям, чем интегральные микросхемы [2.60]. По данным [2.61] 75% всех повреждений микропроцессорных устройств проис-

ходит по причине воздействия перенапряжений. Такие перенапряжения с амплитудой от десятков вольт до нескольких киловольт, возникающие вследствие коммутационных процессов в цепях или при воздействии электростатических разрядов, являются «смертельными» для внутренних микроэлементов микросхем и процессоров. По данным [2.61] обычные транзисторы (дискретные элементы) могут выдерживать напряжение электростатического разряда почти в 70 раз более высокое, чем, например, микрочип памяти (EPROM) микропроцессорной системы. Компьютеризированное промышленное оборудование (в том числе и МУРЗ) особенно уязвимо к действию ЭМИ, так как оно в основном построено на МОП-приборах высокой плотности, которые очень чувствительны к воздействию высоковольтных переходных процессов. Особенностью МОП-приборов является очень малый уровень энергии (напряжения порядка десятков вольт), необходимый для их повреждения или полного уничтожения.

Известны три степени деградации полупроводниковых приборов при воздействии на них мощного ЭМИ: сбой функционирования, устойчивые изменения параметров, катастрофические необратимые отказы. Необратимый выход из строя полупроводников в основном происходит за счет их перегрева или полевого пробоя. [2.62 – 2.64]. Повреждения микропроцессора или элементов памяти, вызванные ослабленными электромагнитными воздействиями, могут носить скрытый характер [2.65]. Такие повреждения не выявляются никакими тестами и могут проявляться в самые неожиданные моменты. Кроме того, под действием ослабленного защитными мерами ПЭМ могут произойти случайные, обратимые сбои, обусловленные самопроизвольным изменением содержания ячеек памяти, называются «мягкими ошибками» (“soft-failures” или “soft errors”). Ошибки такого рода (обратимые, самовосстанавливающиеся нарушения работоспособности) были не известны ранее для электронных устройств, выполненных на дискретных полупроводниковых элементах или на обычных микросхемах.

Прогресс последних лет в области нанотехнологий привел к существенному снижению размеров полупроводниковых элементов (речь идет о единицах и даже долях микрона), уменьшению толщины слоев полупроводниковых и изоляционных материалов, уменьшению рабочих напряжений, увеличению рабочей скорости,

уменьшению электрической емкости отдельных ячеек памяти, увеличению плотности размещения элементарных логических ячеек в одном устройстве. Все это вместе взятое привело к резкому повышению чувствительности элементов памяти к электромагнитным воздействиям. Проблема усугубляется тем, что в современных микропроцессорных структурах наблюдается устойчивая тенденция расширения использования элементов памяти. Многие современные интегральные микросхемы высокого уровня интеграции, входящие в состав микропроцессорного устройства, содержат встроенные элементы памяти достаточно большого объема, исправность которых вообще никак не контролируется. Проблема резкого увеличения чувствительности к электромагнитным воздействиям актуальна не только для элементов памяти, но также и для высокоскоростных логических элементов, компараторов и т. д., то есть, практически, для всей современной микроэлектроники.

Хорошо известно защитное действие от электромагнитных воздействий клетки Фарадея. Здания из железобетона содержат заземленную сетку, реле защиты располагаются в металлических шкафах, сами МУРЗ имеют металлический корпус. Казалось бы – не клетка, а настоящая «матрешка Фарадея». Однако, все не так просто. Во-первых, импульсы высокой частоты свободно проникают сквозь отверстия в клетке Фарадея, сквозь любые неметаллические вставки и окошки, сквозь стеклянные окна зданий и систему вентиляции. При таком частично ослабленном воздействии ЭМИ на полупроводниковые приборы наблюдались случаи частичного разрушения их *p-n*-переходов, что вело к изменениям их характеристик и появлению «мерцающих» сбоев в работе аппаратуры. Такие неисправности связывают значительное количество ресурсов, предназначенных для технического обслуживания и, кроме того, ограничивают уверенность в надежности аппаратуры. Такие «мерцающие» неисправности порой очень сложно выявить, что вызывает необходимость повторного многократного выведения оборудования из эксплуатации со значительными потерями эксплуатационного времени на диагностику повреждений. Этот фактор также должен приниматься во внимание при оценках степени защиты аппаратуры от электромагнитной атаки, так как частичная или неполная защита может привести к дополнительным проблемам.

Вторая проблема известна под названием «запаздывающего действия ЭМИ» и представляет собой очень опасное свойство ПДЭВ. Этот эффект проявляется в течение первых минут после детонации ядерного заряда или заряда электромагнитной бомбы. В это время ЭМИ, проникнув сквозь электрические системы, создает в них локализованные электромагнитные поля. При спадании полей возникают резкие перепады напряжения, которые распространяются в виде волн по проводам систем электропитания на довольно большие расстояния от места возникновения первичного ЭМИ. В-третьих, внешние кабели и провода, выходящие из шкафа релейной защиты (РЗ) и из здания, и тянущиеся на многие километры, практически лишают даже ослабляющего эффекта и здания и шкафы РЗ.

2.9. Основные нормативно-технические документы в области ПЭДВ

В связи с осознанием всей серьезности проблемы ПЭДВ в последние годы этой темой интенсивно занимаются такие организации, как Международная Электротехническая Комиссия (МЭК), СИГРЭ, специальная комиссия при Конгрессе США, Европейские структуры. Совершенно очевидно, что для продуктивной работы в этой области нужны соответствующие стандарты и другая нормативно-техничекая документация. Некоторые из таких стандартов уже разработаны МЭК:

1. **IEC TR 61000-1-3** Electromagnetic compatibility (EMC) — Part 1–3: General—The effects of high-altitude EMP (HEMP) on civil equipment and systems.
2. **IEC 61000-1-5** High power electromagnetic (HPEM) effects on civil systems.
3. **IEC 61000-2-9** Electromagnetic compatibility (EMC)—Part 2: Environment—Section 9: Description of HEMP environment—Radiated disturbance. Basic EMC publication.
4. **IEC 61000-2-10** Electromagnetic compatibility (EMC)—Part 2–10: Environment—Description of HEMP environment—Conducted disturbance.

5. **IEC 61000-2-11** Electromagnetic compatibility (EMC)—Part 2–11: Environment—Classification of HEMP environments.
6. **IEC 61000-2-13** Electromagnetic compatibility (EMC)—Part 2–13: Environment—High-power electromagnetic (HPEM) environments—Radiated and conducted.
7. **IEC 61000-4-23** Electromagnetic compatibility (EMC) - Part 4-23: Testing and measurement techniques - Test methods for protective devices for HEMP and other radiated disturbances.
8. **IEC 61000-4-24** Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 24: Test methods for protective devices for HEMP conducted disturbance - Basic EMC Publication.
9. **IEC 61000-4-25** Electromagnetic compatibility (EMC) - Part 4-25: Testing and measurement techniques - HEMP immunity test methods for equipment and systems.
10. **IEC 61000-4-32** Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium.
11. **IEC61000-4-33** Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters.
12. **IEC 61000-4-35** Electromagnetic compatibility (EMC) - Part 4-35: Testing and measurement techniques - HPEM simulator compendium.
13. **IEC 61000-4-36** Electromagnetic compatibility (EMC) - Testing and measurement techniques - IEMI Immunity Test Methods for Equipment and Systems.
14. **IEC/TR 61000-5-3** Electromagnetic compatibility (EMC)—Part 5–3: Installation and mitigation guidelines—HEMP protection concepts.
15. **IEC/TS 61000-5-4** Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guidelines—Section 4: Immunity to HEMP—Specifications for protective devices against HEMP radiated disturbance. Basic EMC Publication.
16. **IEC 61000-5-5** Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guidelines—Section 5: Specification of protective devices for HEMP conducted disturbance. Basic EMC Publication.

17. **IEC 61000-5-6** Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences.
18. **IEC 61000-5-7** Electromagnetic compatibility (EMC) - Part 5-7: Installation and mitigation guidelines - Degrees of protection provided by enclosures against electromagnetic disturbances (EM code).
19. **IEC 61000-5-8** Electromagnetic compatibility (EMC) - Part 5-8: Installation and mitigation guidelines - HEMP protection methods for the distributed infrastructure.
20. **IEC 61000-5-9** Electromagnetic compatibility (EMC) - Part 5-9: Installation and mitigation guidelines - System-level susceptibility assessments for HEMP and HPEM.
21. **IEC 61000-4-36** Electromagnetic compatibility (EMC) - Testing and measurement techniques - IEMI Immunity Test Methods for Equipment and Systems.

Некоторые из стандартов еще находятся в стадии разработки.

Свой стандарт предлагает и американская ассоциация инженеров электриков IEEE:

IEEE P1642 Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI.

Аналогичный документ разработала и Европейская Комиссия:

Topic SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic (High Power Microwave (HPM)) Attacks.

В СИГРЭ создана отдельная рабочая группа по этой теме:

CIGRE WG C4.206 Protection of the High Voltage Power Network Control Electronics against IEMI.

Много стандартов выпушено Министерством обороны США и НАТО:

1. **MIL-STD-2169B** High –Altitude Electromagnetic Pulse (HEMP) Environmental, 2012.
2. **MIL-STD-188-125-1** High –Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C41 Facilities Performing Critical. Time-Urgent Mission. Part 1 Fixed Facilities, 2005.
3. **MIL-STD-188-125-2** High –Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C41 Facilities Performing Critical. Time-Urgent Mission. Part 2 Transportable Systems, 1999.
4. **MIL-STD-461F** Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 2007.
5. **MIL-STD-464C** Electromagnetic Environmental Effects. Requirements for Systems, 2010. - Test Operations Procedure Report No. 01-2-620 High-Altitude Electromagnetic Pulse (HEMP) Testing.
6. **MIL-STD-1377** Effectiveness of Cable, Connector, and Weapon Enclosure Shielding and Filters in Precluding Hazards of Electromagnetic Radiation to Ordnance (HERO), 1971.
7. **MIL-HDBK-240** Hazards of Electromagnetic Radiation to Ordnance (HERO) Test Guide, 2002.
8. **NATO AECTP-500** Ed. 4. Electromagnetic Environmental Effects Test and Verification, 2011.
9. **NATO AECTP-250** Ed.2 – Electrical and Electromagnetic Environmental Conditions, 2011.

В России опубликовано в открытом доступе лишь несколько официальных документов в этой области:

- **ГОСТ Р 53111-2008** Устойчивость функционирования сети связи общего пользования.
- **РД 45.083-99** Рекомендации по обеспечению стойкости аппаратурных комплексов объектов проводной электросвязи к воздействию дестабилизирующих факторов.
- **ГОСТ Р 52863-2007** Защита информации. Автоматизированные системы в защищенном исполнении испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям.

Первые два документа относятся лишь к узкой области техники – системам связи и основаны на требованиях обычных, а не специальных стандартов по электромагнитной совместимости (ЭМС). Последний документ предназначен для более широкого применения, но также основан на требованиях общих стандартов по ЭМС. Все специальные требования (а это как раз требования по ПЭДВ), обозначены в этом стандарте значком «X» без указания технических параметров, что представляется несколько странным, учитывая название стандарта.

Имеются, естественно, и непубликуемые в открытом доступе материалы, например: «Нормы по стойкости аппаратуры, приборов, устройств и оборудования ЕСС РФ к воздействию ИИ и ЭМИ ЯВ» - Решение ГКЭС при Минсвязи России № 143 от 31.01.96, а также и закрытые (в отличие от западных) военные стандарты. Правда, этот материал имеет весьма узкую область применения, но само по себе его наличие указывает на определенную озабоченность специалистов проблемой ПЭДВ. Хотя, как можно видеть из приведенного выше перечня стандартов, нормы стойкости и методы испытания аппаратуры к воздействию ЭМИ ЯВ уже давно не являются секретными и публикуются на Западе в открытом доступе, причем, как стандарты МЭК общего пользования, так и военные (за редким исключением, например, MIL-STD-2169B). Вряд ли можно признать логичной и оправданной политику России в области чисто технической проблемы, в результате которой большинство российских специалистов во многих областях гражданской техники (например, в области электроэнергетики), так или иначе связанных с проблемами ПЭДВ не имеют о них ни малейшего представления.

В последние годы в России был выполнен целый ряд диссертационных работ, посвященных этой тематике [2.66 – 2.69], правда, все они относятся к воздействию ПЭДВ на системы связи, но это не меняет существа вопроса.

Литература к Главе 2

2.1 Гуревич В. И. Уязвимости микропроцессорных реле защиты. Проблемы и решения. – М.: Инфра-Инженерия, 2014. – 256 с.

2.2 Operation Dominic, Fish Bowl Series, Debris Expansion Experiment. Air Force Weapons Laboratory. Project Officer's Report,

Project 6.7, Report AD-A995 428, POR-2026 (WT-2026), 10 December 1965.
2.3 V. M. Loborev, Up to date state of the NEMP problems and topical research directions, in Euro Electromagnetic Conf. (EUROEM), Bordeaux, France, June 1994, pp. 15-21.
2.4 Kompaneets, A.S., Radio Emission From an Atomic Explosion, Soviet Physics JETP, December 1958.
2.5 W. J. Karzas and R. Latter, Electromagnetic Radiation from a Nuclear Explosion in Space, Physical Review, Vol. 126 (6), pp. 1919-1926, 1962.
2.6 Karzas, W.J., and R. Latter, EMP from High-Altitude Nuclear Explosions, Report No. RM-4194, Rand Corporation, March 1965.
2.7 Karzas, W.J., and R. Latter, Detection of Electromagnetic Radiation from Nuclear Explosions in Space, Physical Review, Vol. 137, March 1965.
2.8 Inston H.H., Diddons R.A. Electromagnetic Pulse Research. - ITT Research Institute Project T1029, Chicago, Illinois 60616, Final Report, September 1965.
2.9 DASA EMP (electronic pulse) Handbook, by United States Defense Atomic Support Agency. Information and Analysis Center, National government publication, Santa Barbara, Calif., 1968.
2.10 Electromagnetic Pulse Problems in Civilian Power and Communications, Summary of a seminar held at Oak Ridge National Laboratory, August 1969, sponsored by the U.S. Atomic Energy Commission and the Department of Defense, Office of Civil Defense.
2.11 EMP Threat and Protective Measures. – Office of Civil Defense, TR-61, August, 1970.
2.12 G. S. Parks, T. I. Dayaharsh, A. L. Whitson, A Survey of EMP Effects During Operation Fishbowl, Defense Atomic Support Agency (DASA), Report DASA-2415, 1970.
2.13 D. B. Nelson, A Program to Counter the Effects of Nuclear Electromagnetic Pulse in Commercial Power Systems, Oak Ridge National Laboratory, Report ORNL-TM-3552 , Part 1. 8, October 1972.
2.14 J. H. Marable, J. K. Baird, and D. B. Nelson, Effects of Electromagnetic Pulse of a Power System, Oak Ridge National Laboratory, Report ORNL-4836, December 1972.

2.15 Sandia Laboratories, “Electromagnetic Pulse Handbook for Missiles and Aircraft in Flight”, SC-M-71 0346, AFWL TR 73-68, EMP Interaction Note 1-1, September, 1972.
2.16 Rickets, L. W., Fundamentals of Nuclear Hardening of Electronic Equipment, Wiley & Sons, Inc., 1972.
2.17 James K. Baird and Nicholas J. Frigo, Effects of Electromagnetic Pulse (EMP) on the Supervisory Control Equipment of a Power System, Oak Ridge National Laboratory, Report ORNL-4899, October 1973.
2.18 L. W. Rickets, J. E. Bridges, J. Miletta, EMP Radiation and Protective Techniques, John Willey and Sons, New York, 1976.
2.19 United States High-Altitude Test Experiences: A Review Emphasizing the Impact on the Environment, Report LA-6405, Los Alamos Scientific Laboratory. October 1976.
2.20 S. Glasstone and P. J. Dolan, The Effects of Nuclear Weapons. U.S. Department of Defense, Washington, DC, 1977.
2.21 C. L. Longmire, On the Electromagnetic Pulse Produced by Nuclear Explosions, IEEE Trans. on Electromagnetic Compatibility, Vol. EMC-20, No. 1, pp. 3-13, February 1978.
2.22 W. Sollfrey, Analytic Theory of the Effects of Atmospheric Scattering on the Current and Ionization Produced by the Compton Electrons from High Altitude Nuclear Explosions, Rand Corp., R-1973-AF, 1977.
2.23 Butler, C., et al., EMP Penetration Handbook for Apertures, Cable Shields, Connectors, Skin Panels, AFWL-TR-77-149, Air Force Weapons Laboratory (The Dikewood Corporation), December 1977.
2.24 HEMP Emergency Planning and Operating Procedures for Electric Power Systems, Oak Ridge National Laboratory, Report ORNL/Sub/91-SG105/1, 1991.
2.25 Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems, Oak Ridge National Laboratory, Report ORNL/Sub/83-43374, 1991.
2.26 HEMP-Induced Transients in Electric Power Substations. Oak Ridge National Laboratory, Report ORNL/Sub-88-SC863, February 1992.

2.27 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Critical National Infrastructures, April 2008.
2.28 High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments. CRS Report for Congress, July 2008.
2.29 The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid, Report Meta-R-320, Metatech Corp., January 2010.
2.30 The Late-Time (E3) High-Altitude. Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid, Report Meta-R-321, Metatech Corp., January 2010.
2.31 Intentional Electromagnetic. Interference (IEMI) and Its Impact on the U.S. Power Grid, Report Meta-R-323, Metatech Corp., January 2010.
2.32 High-Frequency Protection Concepts for the Electric Power Grid, Report Meta-R-324, Metatech Corp., January 2010.
2.33 Protection of High Voltage Power Network Control Electronics Against Intentional Electromagnetic Interference (IEMI), Report CIGRE Working Group C4.206, November 2014.
2.34 IEC TR 61000-1-3 Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems.
2.35 IEC 61000-2-9 Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance. Basic EMC publication.
2.36 IEC 61000-2-10 Electromagnetic compatibility (EMC) - Part 2-10: Environment - Description of HEMP environment - Conducted disturbance.
2.37 IEC 61000-2-11 Electromagnetic compatibility (EMC) - Part 2-11: Environment - Classification of HEMP environments.
2.38 IEC 61000-2-13 Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted.
2.39 IEC/TR 61000-5-3 Electromagnetic compatibility (EMC) - Part 5-3: Installation and mitigation guidelines - HEMP protection concepts.

2.40 IEC/TS 61000-5-4 Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 4: Immunity to HEMP - Specifications for protective devices against HEMP radiated disturbance. Basic EMC Publication.
2.41 IEC 61000-5-5 Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 5: Specification of protective devices for HEMP conducted disturbance. Basic EMC Publication.
2.42 IEEE P1642 Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI.
2.43 Topic SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic (High Power Microwave (HPM)) Attacks, European Commission Security Research Program , 2010.
2.44 MIL-STD-188-125-1. High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C^4I Facilities Performing Critical Time-Urgent Missions, Department of Defense, 1994.
2.45 MIL-STD-461E. Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, Department of Defense, 1993.
2.46 MIL-STD-464C. Electromagnetic Environmental Effects Requirements for Systems, Department of Defense, 1997.
2.47 MIL-STD-2169B. High Altitude Electromagnetic Pulse (HEMP) Environment, Department of Defense, 1993.
2.48 MIL-Hdbk-423. Military Handbook: High Altitude Electromagnetic Pulse (HEMP) Protection for Fixed and Transportable Ground-Based C41 Facilities, Vol. 1: Fixed Facilities Department of Defense, 1993.
2.49 High Altitude Electromagnetic Pulse (HEMP) Testing, Test Operations Procedure 01-2-620, U. S. Army Test and Evaluation Command, 2011.
2.50 Гуревич В. И. Повышение устойчивости энергосистем к преднамеренным электромагнитным деструктивным воздействиям – актуальная задача современности. – Энергоэксперт, 2015.
2.51 Белоус В. Угроза использования ЭМИ оружия в военных и террористических целях. – Ядерный контроль, 2005, № 1 (75), том 11, с. 133 – 140.

2.52 Буралков А. А., Кибардин В. В. О влиянии солнечных бурь на надежность энергосистем. – Тезисы докладов Международного научно-технического конгресса «Энергетика в глобальном мире», Красноярск, 16-18 июня 2010, стр. 32-33.

2.53 Грехов И.В., Ефанов В.М., Кардо-Сысоев А.Ф., Шендерей С.В. Формирование высоковольтных наносекундных перепадов напряжения на полупроводниковых диодах с дрейфовым механизмом восстановления. // Письма в ЖТФ. 1983. Т. 9. Вып. 7. С. 435-439.

2.54 Тучкевич В.М., Грехов И.В. Новые принципы коммутации больших мощностей полупроводниковыми приборами. Л.: Наука. 1988. 117 С.

2.55 Грехов И.В. Импульсная коммутация больших мощностей полупроводниковыми приборами. В кн.: Физика и техника мощных импульсных систем / Под ред. Е.П. Велихова. М.: Энергоатомиздат, 1987. С. 237.

2.56 Слюсар В. Генераторы супермощных электромагнитных импульсов в информационных войнах. – Электроника: Наука, техника, бизнес 2002 , Вып. 5, с. 60- 67.

2.57 Словиковский Б. Г. Малогабаритные генераторы высоковольтных наносекундных импульсов на основе SOS-диодов. Автореферат диссертации на соиск. ст. канд. техн. наук., Екатеринбург, 2004.

2.58 Гуревич В. И. Оптоэлектронные трансформаторы: панацея или частное решение частных проблем. - "Вести в электроэнергетике", 2010, № 2, с. 24 - 28.

2.59 Киричек Р. В. Исследование влияния сверхкоротких электромагнитных импульсов на процесс передачи данных в сетях Ethernet. – Автореферат дисс. канд. техн. наук, 05.12.13, СПб, 2011.

2.60 Гуревич, В. Надежность микропроцессорных устройств релейной защиты: мифы и реальность. – Проблемы энергетики. – 2008. – №5-6. – С. 47-62.

2.61 Clark O. M., Gavender R. E. Lighting Protection for Microprocessor-based Electronic Systems. IEEE Transactions on Industry Applications, vol. 26, No. 5, 1990.

2.62 Блудов С.Б., Гадецкий Н.П., Кравцов К.А. и др. Генерирование мощных СВЧ-импульсов ультракороткой длительности и

их воздействие на изделия электронной техники. Физика плазмы, 1994, том 20, N 7, 8, с. 712- 717.

2.63 Панов В.В., Саркисьян А.П. Некоторые аспекты проблемы создания СВЧ-средств функционального поражения. Зарубежная радиоэлектроника, 1993, 10, 11, 12, стр. 3-10.

2.64 Антипин В.В., Годовицын В.А., Громов Д. В. , Кожевников А. С., Раваев А.А. Влияние мощных импульсных микроволновых помех на полупроводниковые приборы, интегральные микросхемы. Зарубежная радиоэлектроника, 1995, 1, стр. 37-53.

2.65 Phadke A. G. Hidden failures in electric power systems. International Journal of Critical Infrastructures, vol. 1, No. 1, 2004.

2.66 Методы обеспечения стойкости перспективных систем радиорелейной, тропосферной и спутниковой связи к воздействию мощных импульсных электромагнитных помех / Воскобович Владимир Викторович — 05.12.13 — Москва, 2002.

2.67 Разработка методов оценки стойкости телекоммуникационных систем к воздействию сверхширокополосных электромагнитных импульсов / Ведмидский Александр Александрович — 05.12.13 — Москва, 2003.

2.68 Теоретические и экспериментальные методы оценки устойчивости терминалов к воздействию сверхширокополосных электромагнитных импульсов / Акбашев, Беслан Борисович — 05.12.13 — Москва, 2005.

2.69 Методы и средства оценки воздействия электромагнитного импульса большой энергии на телекоммуникационные сети / Якушин Сергей Павлович — 05.12.13 — Москва, 2004.

3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ МУРЗ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

3.1. Чувствительность МУРЗ к электромагнитным воздействиям

Проблема электромагнитной совместимости электронной аппаратуры (ЭМС) возникла вместе с самой этой аппаратурой, поскольку одни ее узлы функционально построены таким образом, что являются приемниками электромагнитного излучения, тогда как другие – источниками излучения. Проблемы возникали как из-за взаимного влияния одних узлов на другие внутри аппаратуры, так и при воздействии на электронную аппаратуру внешних излучений различного происхождения. Десятилетиями проблемы ЭМС были прерогативой специалистов в области электроники, радиотехники, связи. Неожиданно, в последние 15 – 20 лет, эта проблема стала весьма актуальной и в электроэнергетике. Конечно, довольно значительные электромагнитные поля на объектах электроэнергетики существовали всегда. Однако, применявшиеся десятилетиями устройства автоматики, управления и релейной защиты электромеханического типа были мало подвержены этим полям и никаких особых проблем с ЭМС не возникало. Последние два десятилетия характеризуются интенсивным переходом от электромеханических к микропроцессорным устройствам релейной защиты (МУРЗ) и автоматики в электроэнергетике. Причем, переход этот осуществляется не только по мере строительства новых подстанций и электростанций, но и путем замены старых электромеханических реле защиты (ЭМЗ) на старых подстанциях, построенных еще в те времена, когда никто даже не предполагал использование на них микропроцессорной техники, на суперсовременные МУРЗ. Последние оказались весьма чувствительными к электромагнитным помехам, поступающим «из воздуха», по цепям оперативного тока, цепям напряжения и трансформаторов тока. Отмечались случаи ложного срабатывания МУРЗ даже от мобильного телефона [4.1] и не только. Другие характерные примеры - случаи ложного срабатывания микропроцессорных устройств на действующих объектах "Мос-

энерго", Очаковской и Зубовской подстанциях. Алгоритм работы защит нарушался из-за молнии, работающего по близости экскаватора, электросварки и некоторых других помех. Во время ввода в действие Липецкой подстанции, которая потратила около полутора миллионов долларов на приобретение МУРЗ, проблемы с микропроцессорными устройствами полгода не позволяли запустить этот энергообъект. В итоге подстанцию запускали, используя комплект традиционных защит [4.2]. На практике приходилось сталкиваться со случаями, когда, например, короткие замыкания по стороне 110 кВ вызывали ложную работу защит по стороне 330 кВ, а помехи при коммутациях по одному классу напряжений проникали (через общие цепи оперативного тока) на входы аппаратуры РЗА, работающей по другому классу напряжения [4.3].

Неправильная работа релейной защиты по причине недостаточной ЭМС, по данным «Мосэнерго», составляет до 10% от всех случаев ложной работы и касается в основном только реле на микроэлектронной и микропроцессорной элементной базе [4.4]. Столь высокий процент случаев неправильной работы по причине недостаточной ЭМС вызван тем, что чувствительность к электромагнитным помехам МУРЗ на несколько порядков выше, чем у традиционных электромеханических защит. Например, по данным [4.4] если для нарушения работы электромеханического реле требуется энергия 10^{-3} джоуля, то для нарушения работы интегральных микросхем требуется всего 10^{-7} джоуля. Разница составляет 4 порядка или 10000 раз.

Степень повреждения зависит от устойчивости как каждого из компонентов схемы, так и от энергии мощной помехи в целом, которая может быть поглощена схемой без появления дефекта или отказа. Например, для электромагнитного реле с катушкой на напряжение 230 В переменного тока коммутационная помеха от индуктивной нагрузки с амплитудой 500 В хотя и является более чем двукратным перенапряжением, но вряд ли приведет к отказу реле в силу стойкости электромеханики к такого рода помехам и вследствие малой длительности такой помехи (в течение микросекунд). Иначе обстоит дело с микросхемой, питающейся от источника 5 В постоянного тока. Импульсная помеха с амплитудой 500 В в сто раз превышает напряжение питания этого электронного компонента и приводит к неизбежному отказу и последующему разруше-

нию устройства. Стойкость микросхем к перенапряжениям на несколько порядков ниже, чем электромагнитного реле [4.5]. Импульсные перенапряжения, возникающие при разрядах молний и при коммутации в силовых электроустановках, способны повреждать и разрушать как электронные устройства, так и целые системы. Многолетняя статистика подтверждает, что число таких повреждений удваивается каждые три-четыре года [4.5]. Эта статистика хорошо согласовывается с так называемым Законом Мора [4.6], еще в 1965 году показавшем, что количество полупроводниковых компонентов в микрочипах удваивается примерно каждые два года и такая тенденция сохраняется уже много лет. Если каких-то десять лет тому назад микросхемы так называемой транзисторно-транзисторной логики (TTL) содержали 10-20 элементов на квадратный миллиметр и имели типичное напряжение питания 5 В, то сегодня популярные микросхемы могут содержать почти сто CMOS (Complementary Metal-Oxide Semiconductor) транзисторов на каждом квадратном миллиметре поверхности и имеют напряжение питания только 1.2 В. Новейшие технологии твердого тела, например, SOS (Silicon-On-Sapphire), поднимают плотность элементов до 500 на одном квадратном миллиметре поверхности [4.7]. Очевидно, что для таких микросхем потребуется еще более низкое напряжение питания. При этом совершенно очевидно, что с повышением степени интеграции в микроэлектронике уменьшается устойчивость ее компонентов к высоковольтным импульсным перенапряжениям по причине уменьшения толщины изоляционных слоев и уменьшения рабочих напряжений полупроводниковых элементов.

Поскольку помехи, имеющие меньшую энергию, возникают чаще помех, имеющих большую энергию, наиболее частой реакцией МУРЗ на воздействие электромагнитных помех будет не разрушение устройства, а нарушение его работы или кратковременный сбой в работе с последующим восстановлением нарушенной функции, рис. 3.1.

Это означает, что сработавшее не правильно на подстанции МУРЗ покажет полностью исправную работу при его исследовании в лаборатории и установить причину его ложного срабатывания на подстанции будет невозможно. Статистика, собранная представителями крупнейших Японских компаний-производителей МУРЗ ярко подтверждает эту особенность МУРЗ, рис. 3.2 [4.8] .

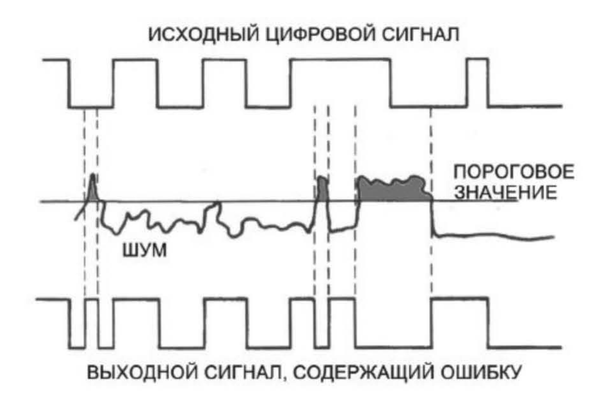


Рис. 3.1. Воздействие помехи малой энергии на работу цифрового устройства

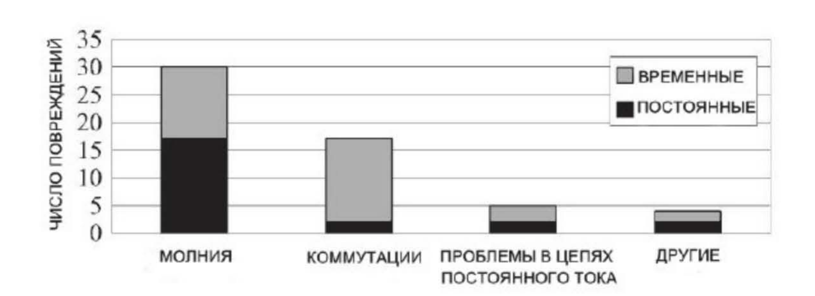


Рис. 3.2. Данные Японских компаний-изготовителей по повреждамости МУРЗ от электромагнитных воздействий

Как видно из представленной диаграммы, кратковременные не повторяющиеся нарушения функционирования (сбои в работе) МУРЗ являются превалирующими в большинстве случаев. Этот вывод подтверждается также и данными, полученными другой группой исследователей [4.9]. Согласно их данным, нарушения функционирования такого рода составляют почти 70 % от общего числа

повреждений МУРЗ, причем, до 80% этих сбоев происходит в интегральных микросхемах.

По свидетельству [4.4] и в практике ОАО «Мосэнерго» накопилось уже достаточно подтверждений негативного влияния электромагнитных помех на работу МУРЗ. Наиболее наглядно это показывает опыт включения МП защит фирмы «SIEMENS» на ТЭЦ-12 ОАО «Мосэнерго» по проекту, выполненному институтом «Атомэнергопроект». При проектировании никак не были учтены требования ЭМС. Вследствие помех только за период с августа по декабрь 1999 года было зарегистрировано более 400 ложных информационных сигналов по дискретным и аналоговым входам МУРЗ [4.4]. При этом следует иметь в виду, что стоимость каждого отказа МУРЗ раз в 10 выше, чем стоимость отказа одного электромеханического реле вследствие концентрации большого количества функций в каждом МУРЗ.

Помехи, проникающие по кабелям на входы электронной аппаратуры, называются «кондуктивными». Кроме помех такого вида, импульс сильного тока, проходящий по проводам и кабелям, создает и помехи в виде электромагнитных полей, воздействующих на все близко расположенные проводники. Такое воздействие называется «индуктивным». Существуют еще и емкостные наводки, при которых короткие (то есть высокочастотные) импульсы перенапряжения из высоковольтных линий электропередач попадают в низковольтные цепи через емкостные связи между обмотками трансформаторов.

В процессе распространения помехи имеет место многократное превращение одного его вида в другой, поэтому такое деление весьма условно, особенно, когда речь идет о высокочастотных процессах. Более того, попав в электронную аппаратуру посредством электромагнитного поля или по проводам, помеха претерпевает многочисленные превращения уже внутри этой аппаратуры из-за наличия паразитных емкостных и индуктивных связей между отдельными элементами или между различными узлами аппаратуры. При этом, высокочастотная составляющая помехи может проникать вглубь аппаратуры, в обход установленных фильтров и защитных элементов. Еще один путь для проникновения помехи: протекание токов по заземленному металлическому корпусу МУРЗ и по заземленным экранам многочисленных кабелей, подключенных к нему.

Все это говорит о том, что обеспечить должный уровень защиты от электромагнитных помех электронной аппаратуры очень и очень не просто даже когда речь идет о помехах естественного, а не искусственного происхождения. Если же говорить о защите электронной аппаратуры от ПЭДВ, в частности от ЭМИ ЯВ, то проблема становится еще более сложной, а ее решение более дорогостоящим. Тем не менее, очень важно подчеркнуть, что решив проблему защиты от ПЭДВ, мы обеспечим более надежную работу электронной аппаратуры подстанций и в обычных режимах работы, то есть при воздействии естественных помех.

3.2. Методы защиты от ПЭДВ

Методы защиты электронной аппаратуры подстанций от ПЭДВ могут быть разделены на пассивные, активные и организационно-технические.

Пассивные методы защиты подразумевают использование дополнительных внешних средств (технологий, материалов, элементов и т.п.) не связанных непосредственно с алгоритмом и режимом работы защищаемого оборудования. Они включают в себя специальные монтажные шкафы и специальные экранированные кабели, ограничители перенапряжений и фильтры, улучшенные системы заземления, специальные строительные материалы, краски, лаки, пленочные покрытия, металлизированные коврики и шторы и, наконец, использование специальных элементов и материалов в конструкции самой электронной аппаратуры.

Активные методы защиты подразумевают использование внешних устройств, алгоритм работы которых непосредственно связан с алгоритмом и режимом работы защищаемого оборудования. На примере МУРЗ можно показать, что к таким методам защиты могут быть отнесены специально разработанные упрощенные пусковые органы релейной защиты, выполненные на электромеханической основе и обладающие повышенной устойчивостью к ПЭДВ. Такие пусковые органы не реагируют на короткий ЭМИ и не могут быть им повреждены, однако реагируют на один из параметров аварийного режима (ток, напряжение) и вводят в работу МУРЗ, который обеспечивает реализацию всего набора необходимых характеристик.

Организационно-технические мероприятия включают организацию и технические средства специального хранения запасных частей (ЗИПа) электронной аппаратуры, обеспечивающего максимально быстрое восстановление поврежденной аппаратуры, стандартизацию конструкции и программного обеспечения электронного оборудования, в частности МУРЗ, обеспечивающую взаимозаменяемость внутренних блоков и модулей, универсализацию методов проверки исправности электронной аппаратуры специальными тестовыми системами, сокращающую время восстановления работоспособности аппаратуры.

При выборе и практическом использовании средств защиты от воздействия ЭМИ всегда следует иметь виду, что только один из видов защит не в состоянии обеспечить эффективную защиту. И лишь совместное, комплексное использование различных методов и средств защиты может обеспечить надежную защиту электронной аппаратуры. Так, например, использование специального защищенного от ЭМИ монтажного шкафа не защищает чувствительную аппаратуру от проникновения ЭМИ по проводам, входящим в этот шкаф и подключенным к входам этой аппаратуры. Точно так же, как и использование специальных фильтров, защищающих от проникновения ЭМИ через провода, не защищают от электромагнитного излучения, проникающего в аппаратуру через окна и вырезы в ее корпусе. А использование защищенных монтажных шкафов и фильтров не решает проблем, связанных с воздействием ЭМИ на аппаратуру через систему заземления.

4. ПАССИВНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ МУРЗ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

4.1. Монтажные шкафы

Рис. 4.1. Монтажный шкаф с усиленной защитой от ЭМИ, снабженный специальными петлями, прокладками из электропроводной резины, специальными стыковочными и соединительными элементами, экранированными вентиляционными окнами и т.д. (Equipto Electronics Corp.)

Идеальной защитой от ЭМИ явилось бы полная изоляция электронной аппаратуры от внешнего мира и укрытие помещения, в котором она размещена сплошным толстостенным ферромагнитным экраном. Вместе с тем ясно, что практически реализовать такую защиту для МУРЗ невозможно.

Поэтому на практике приходится использовать менее надежные средства защиты, такие, как токопроводящие сетки или пленочные токопроводящие покрытия для окон, сотовые металлические конструкции для воздухозаборников и вентиляционных отверстий и специальные электропроводные смазки и прокладки из электропроводной резины, размещаемые по периметру дверей и люков.

Сегодня на рынке широко представлены металлические шкафы, рис. 4.1, специальной конструкции, обеспечивающие существенное ослабление электромагнитного излучения. Стандартные шкафы из обычной листовой стали, не содержащие окон или щелей, уже существенно ослабляют ЭМИ. Однако, использование оцинкованных монтажных панелей для изготовления шкафов, а также специальных электропроводных уплотнителей и прокладок существенно по-

вышают эффективность таких шкафов, поскольку покрытие цинком позволяет выровнять потенциалы на большой площади (удельное сопротивление стали 0.103-0.204 Ом x мм^2/м, а удельное сопротивление цинка 0.053-0.062 Ом x мм^2/м). Еще более низким сопротивлением (0,028 Ом x мм^2/м) обладает алюминий. Поэтому некоторые компании выполняют моноблочные шкафы из специального сплава ALUZINC 150 (Aluzinc® -(зарегистрированная торговая марка концерна Arcelor) – это сталь имеющая покрытие, на 55% состоящее из алюминия, на 43,4% из цинка и на 1,6% из кремния.) Поверхность шкафа, содержащая такое покрытие, обеспечивает высокую степень отражения электромагнитного излучения. Шкафы из такого материала производит и поставляет во многие страны компания Sarel (сегодня - Schneider Electric Ltd., Великобритания) Аналогичные шкафы, предназначенные для защиты от ЭМИ, выпускаются сегодня и другими компаниями: Canovate Group, R.F. Installations, Inc.; Universal Shielding Corp.; Eldon; Equipto Electronics Corp.; ATOS; MFB; European EMC Products Ltd; Amco Engineering; Addison и многими другими. Такого рода шкафы обычно ослабляют излучение на 80-90 дБ на частотах 100 кГц – 1 ГГц.

Проблема заключается в том, что в реальной ситуации монтажные шкафы для релейной защиты неизбежно будут иметь многочисленные отверстия для ввода и вывода десятков кабелей, что неизбежно приведет к снижению эффективности экранирования. Кроме того, МУРЗ, расположенные внутри такого шкафа, а также сами шкафы должны быть заземлены. Однако, существующая на подстанциях система заземления далеко не лучшим образом реагирует на воздействие ЭМИ ЯВ и, вопреки ожиданиям, не способствует защите электронной аппаратуры от этого воздействия.

4.2. Заземление чувствительной электронной аппаратуры

“Заземление является самой плохо понимаемой темой в автоматизации… Решение проблем заземления в настоящее время находится на грани между пониманием, интуицией и везением”

Виктор Денисенко
докт. техн. наук, Главный конструктор
Научно-исследовательской лаборатории автоматизации проектирования

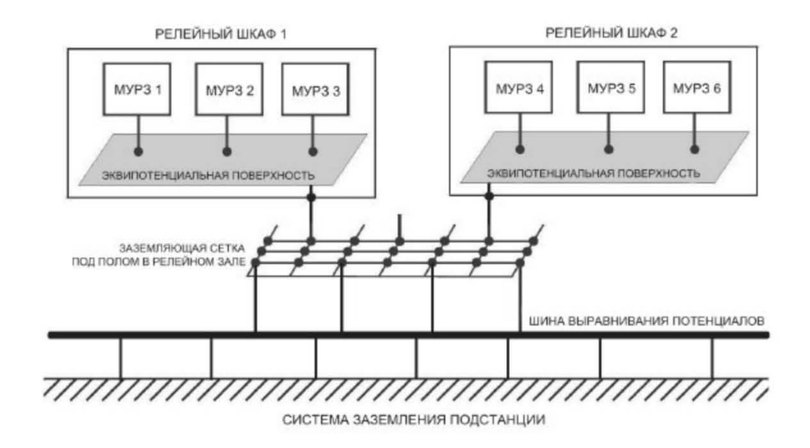


Рис. 4.2. Схема многоточечного заземления МУРЗ с использованием эквипотенциальной поверхности

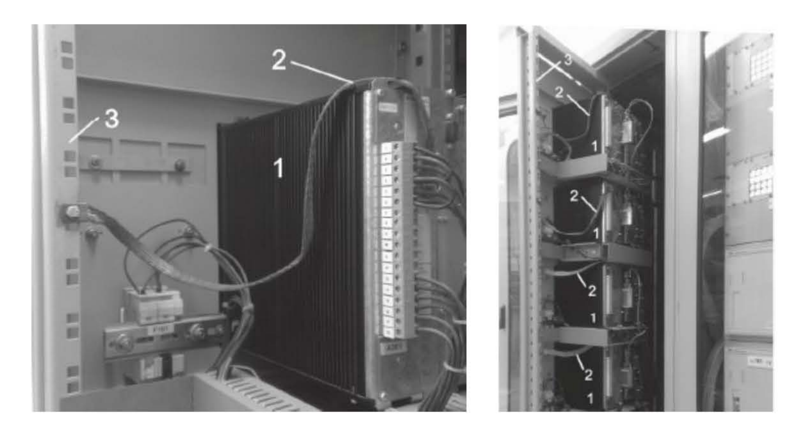


Рис. 4.2. Устройство заземления МУРЗ, установленных в металлических шкафах, с использованием эквипотенциальной поверхности. 1 – МУРЗ в металлических корпусах; 2 – заземляющие медные шинки; 3 – элемент конструкция металлического шкафа, выполняющего роль эквипотенциальной поверхности

Современная, считающаяся правильно спроектированной система заземления МУРЗ выполняется многоточечной с использованием эквипотенциальной поверхности, рис. 4.2. В качестве эквипотенциальной поверхности могут использоваться металлические элементы конструкций релейных шкафов, рис. 4.3.

К сожалению, на объектах электроэнергетики (подстанциях и электростанциях), имеющих значительную территорию, даже такие, методы заземления не являются достаточно эффективными, ввиду неизбежности заземление различных электроустановок, расположенных на большом удалении друг от друга, в различных точках общего контура заземления. При этом, эти точки заземления приобретают значительную разность потенциалов в момент протекании больших импульсных токов через контур заземления. Если эти электроустановки не имеют между собой гальванической связи, например, как реле защиты, соединенные между собой волоконно-оптическими линиями связи (ВОЛС), то эта разность потенциалов особой роли не играет. Но, если реле защиты, расположенные на удалении друг от друга, соединены между собой посредством проводной системы связи (то есть витой парой и обычным каналом связи Ethernet, на который в последнее время переходят с целью удешевления систем электроснабжения), то к низковольтным узлам этой системы связи окажется приложенным высокое напряжения, которое неизбежно приведет к повреждению этой системы, то есть, во многих случаях, к отказу релейной защиты, рис. 4.4.

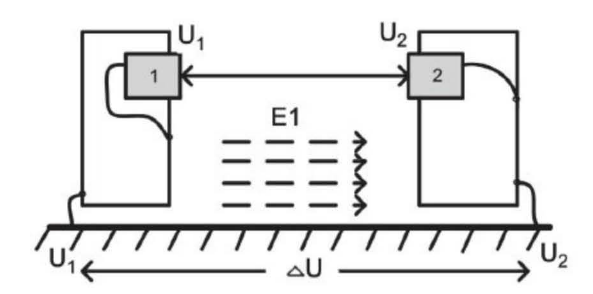


Рис. 4.4. Схема подключения двух МУРЗ (1 и 2), расположенных на значительном расстоянии друг от друга, с неизолированным каналом связи (витая пара и сеть Ethernet)

По свидетельству [4.1]: «*чем больше площадь территории защищаемого объекта, тем больший потенциал для проблем*».

Как известно, существует два вида заземления: так называемое функциональное (или рабочее) и защитное. Как следует уже из названий этих видов заземления, первое из них предназначено лишь для обеспечения нормального функционирования (работы) оборудования (ПУЭ 1.7.30), а второе – исключительно для обеспечения электробезопасности персонала (ПУЭ 1.7.29). В [4.2] утверждается, что функциональное заземление необходимо для обеспечения работоспособности МУРЗ и рассматриваются различные варианты выполнения такого заземления и методы его испытания. Действительно, на некоторых печатных платах МУРЗ имеются зачищенные и покрытые слоем серебра участки печатных проводников, увеличенной ширины, которые при установке платы в корпусе приходят в соприкосновение со специальными пружинами, обеспечивающими контакт этих печатных проводников с заземленным корпусом МУРЗ, рис. 4.5.

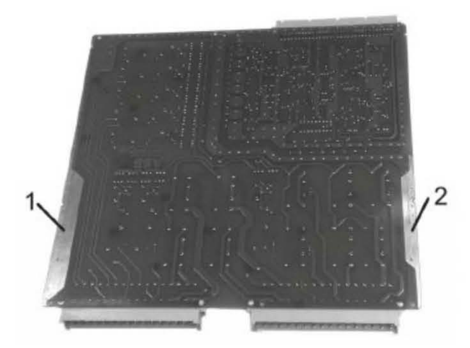


Рис. 4.5. Печатная плата МУРЗ с зачищенными участками печатного монтажа (1 и 2), контактирующими с заземленным корпусом посредством специальной пружины

Но действительно ли функциональное заземление необходимо для нормальной работы МУРЗ, все входные и выходные цепи которого хорошо изолированы от земли и от других электроустановок (при использовании ВОЛС для связи между терминалами)? Ведь работоспособность внутренних электронных цепей МУРЗ никак не

связана с наличием или отсутствием заземления. Что же касается эффективности защиты чувствительных электронных цепей МУРЗ от воздействия внешних электромагнитных полей с помощью металлического корпуса, призванного выполнять роль так называемой «клетки Фарадея», то эта эффективность никак не зависит от наличия или отсутствия заземления. То есть заземление корпуса МУРЗ никак не влияет на эффективность экранирующего эффекта корпуса. С другой стороны, если сигналы помех поступают на электронные цепи МУРЗ, расположенные внутри корпуса, по кабелям, то каким образом заземление его корпуса предотвратит воздействие этих помех (особенно помех дифференциального типа)? Ответ очевиден: никак! Более того, можно утверждать, что заземление корпусов МУРЗ лишь усугубляет ситуацию и снижает помехоустойчивость релейной защиты. Так, например, в соответствии со стандартом IEC 60255-22-4 импульсным напряжением наносекундного диапазона с амплитудой 4 кВ проверяются все входные и выходные цепи реле защиты, за исключением портов цифровой связи. То есть, заранее предполагается, что эти порты и цепи не выдержат таких испытаний. Но при использовании обычной витой пары и присоединения этих цепей к сети Ethernet вместо использования ВОЛС, к этим цепям неизбежно будет приложено высокое напряжение в случае, изображенном на рис. 4.4. А как изменится ситуация, если корпуса МУРЗ будут тщательно изолированы от системы заземления? Если пренебречь паразитными емкостями (а в рассмотренном ниже варианте конструктивного исполнения ими действительно можно будет пренебречь), то исходя из того же рис. 4.4, к портам цифровой связи высокое напряжение приложено не будет.

Еще одна проблема принятой сегодня системы заземления - электромагнитный импульс высотного ядерного взрыва (ЭМИ ЯВ), в частности, его так называемая «быстрая» составляющая – E1, которая характеризуется коротким, но очень мощным импульсом электрического поля у поверхности Земли, напряженностью до 50 кВ/м с передним фронтом около нескольких наносекунд и задним фронтом около одной микросекунды [4.3]. Это поле имеет сложную структуру и содержит вертикальную и горизонтальную составляющие, которые обуславливают появление значительных импульсов тока в протяженных проводниках, в частности, в системах заземления, выполняющих роль больших антенн, абсорбирующих электро-

магнитную энергию на большой площади. В случае разряда молнии или пробоя изоляции высоковольтного электрооборудования, имеющего функционально заземленные части (например, заземленные нулевые точки обмоток высоковольтных трансформаторов, соединенных в звезду) система заземления выполняет роль электрода, имеющего нулевой потенциал. В большинстве нормативных документов, даже таких серьезных, как [4.4], не делается никакой разницы между воздействием на систему заземления разряда молнии и компонента Е1 ЭМИ ЯВ. Например, в документе [4.4] дословно записано следующее: “*Так как влияние наведенной электромагнитным импульсом помехи подобно той, что наблюдается при разрядах молнии, система молниеотводов и система заземляющих электродов - главные интерфейсы системы защиты от электромагнитного импульса*”.

Однако, на самом деле имеется существенная разница между высоковольтным разрядом молнии на систему заземления, имеющую нулевой потенциал или пробоем изоляции высоковольтного оборудования на землю и импульсом Е1 мощного электрического поля, часть которого направлена параллельно поверхности земли (то есть параллельно сетке системы заземления. При возникновении ЭМИ ЯВ система заземления уже перестает исполнять роль поверхности с нулевым потенциалом и начинает играть роль источника высокого импульсного напряжения, прикладываемого к электрооборудованию, заземленному в различных частях системы заземления и имеющих гальваническую связь между собой, рис. 4.4. Поскольку речь идет об очень мощном и очень коротком (то есть имеющем высокочастотные свойства) импульсе, создающем в воздухе напряженность поля, достигающую 50 кВ/м, то становится понятным, что даже на небольшом участке стандартной системы заземления может появиться очень высокая разность потенциалов, намного превышающая значение, возникающее при протекании токов молнии через систему заземления. Поэтому, требования к электрической прочности изоляции входных и выходных цепей МУРЗ выдерживать испытательные импульсные напряжения наносекундного диапазона с амплитудой 4 кВ, указанные в стандарте IEC 60255-22-4, уже явно не достаточны для обеспечения работоспособности МУРЗ. Кроме того, мы неспроста упомянули выше о корпусе МУРЗ как об элементе, «призванном выполнять роль «клетки

Фарадея», а не «выполняющего роль «клетки Фарадея». Потому, что на самом деле металлические корпуса современных МУРЗ довольно плохо справляются с ролью «клетки Фарадея» из-за наличия в них больших вырезов для экранов, кнопочных панелей, клеммных колодок, рис. 4.6.

Рис. 4.6. Современные терминалы МУРЗ в корпусах с многочисленными окнами, вырезами и отверстиями под экраны, кнопки, индикаторные панели и другие элементы

Параметры составляющей Е1 ЭМИ ЯВ таковы, что все эти вырезы в металлическом корпусе обуславливают проникновения мощной электромагнитной волны с эквивалентной частотой доходящей до десятков гигагерц, во внутрь корпуса МУРЗ.

Стандартные металлические шкафы, в которых сегодня размещаются комплекты устройств релейной защиты, также мало пригодны для защиты МУРЗ от высокочастотных электромагнитных полей, поскольку имеют полностью открытую нижнюю (или верхнюю) часть для ввода многочисленных кабелей, а иногда и стеклянные двери через которые удобно наблюдать за экранами и индикаторами МУРЗ, не открывая их, рис. 4.7. Поэтому так или иначе, необходимо искать альтернативные решения для обеспечения такой защиты. Таким образом, становится очевидным, что действительно необходимым является лишь защитное заземлении корпусов МУРЗ, предохраняющее персонал от поражения электрическим током при

прикосновении к корпусу МУРЗ, но никак не функциональное заземление.

Рис. 4.7. Терминалы МУРЗ, установленные в стандартных шкафах со стеклянными дверями

Что касается защиты от воздействия компонента E1 ЭМИ ЯВ, то оказывается, что известные технические решения по системам заземления, применяемые в электроэнергетике, являются не просто бесполезными из-за высокого сопротивления на эквивалентной частоте в десятки гигагерц, но и опасными для чувствительной электронной аппаратуры. Таким образом, требование заземления корпусов микропроцессорных устройств релейной защиты, приходит в противоречие с требованием обеспечения их устойчивости к воздействию ЭМИ ЯВ.

По утверждению [4.2] функциональное заземление невозможно рассматривать в отрыве от защитного заземления, не нарушая стандартов системы безопасности труда. Позволим себе усомниться в справедливости такого утверждения и рассматривать эти два вида заземления как отдельные и независимые друг от друга. При таком подходе появляется возможность организации заземления МУРЗ на новом принципе, который основан на рекомендации IEC 60364-5-

548 [4.5] о повышении помехоустойчивости оборудования информационных технологий путем отделения этого оборудования от источников возмущения.

Поскольку в рассматриваемом случае таким «источником возмущения» является функциональное заземление, то наше предложение заключается в отделении МУРЗ от него, рис. 4.8.

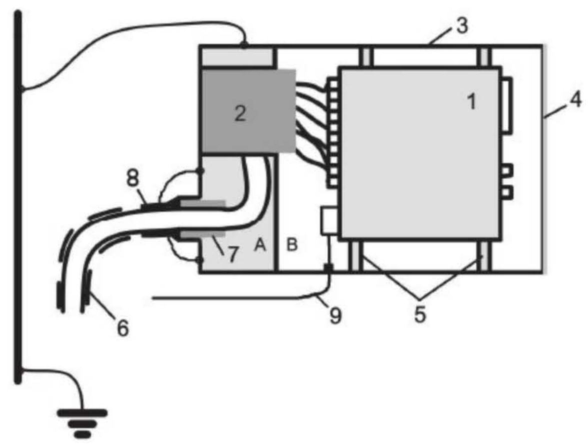


Рис. 4.8. Предлагаемый принцип компоновки МУРЗ, обеспечивающий повышенную устойчивость ко всем видам электромагнитных воздействий, включая ЭМИ ЯВ

А – «грязный» отсек; В – «чистый» отсек; 1 – терминал МУРЗ в тщательно изолированном пластмассовом корпусе; 2 – фильтр ЭМИ ЯВ; 3 – стальной корпус; 4 – дверца стального корпуса; 5 – изоляторы; 6 – контрольный кабель с двойным экраном; 7 – проходной изолятор; 8 – металлическая муфта для сочленения оплетка кабеля со стальным корпусом; 9 – оптоволоконная линия связи

Согласно этому предложению, стальной контейнер 3, рис. 4.8, с минимальным количеством отверстий разделен внутренней переборкой на две зоны: А - «грязную» и В - «чистую». Терминал МУРЗ в пластмассовом корпусе размещен в чистой зоне, свободной от электромагнитных излучений. Контейнер 3 снабжен дверцей 4, обеспечивающей доступ персонала к лицевой панели МУРЗ во время профилактических работ. Контейнер 3 заземлен с соблюдением

всех традиционных норм и правил выполнения заземления, что обеспечивает соблюдение требований техники безопасности. При наличии достаточно большого расстояния между МУРЗ и внутренними стенками заземленного металлического контейнера, например, 5 - 7 см, паразитная емкость электронных цепей МУРЗ на землю будет очень незначительной и ее влиянием можно пренебречь. Что касается самого корпуса МУРЗ, то он должен быть тщательно изолированным (выполненным из пластмассы), с принятием дополнительных мер по предотвращению выноса опасного потенциала на поверхность этого корпуса. Такими мерами могут быть: закрытие экрана дополнительной прозрачной пластмассовой панелью; вывод управляющих кнопок на поверхность корпуса через изоляционные проставки; подвод света со светодиодов на световое табло, расположенное на поверхности корпуса, через жесткие пластмассовые световоды; использование изолированного оптического порта для подключения внешнего компьютера к МУРЗ. В общем, это такие же простые приемы обеспечения безопасности, которые приняты при отсутствии заземления в ручных электроинструментах с так называемой двойной изоляцией и не представляют никакой особой сложности в их практической реализации.

Что касается снятия возможного электростатического заряда, который может накопиться на изолированном корпусе МУРЗ, то эта проблема может быть решена нанесением тонкого высокоомного полупроводящего покрытия на внутреннюю поверхность пластмассового корпуса и соединением ее с заземленным стальным корпусом через специальный высоковольтный (50 – 100 кВ) высокоомный (около 50 МОм) резистор. Электростатический заряд будет стекать на землю через такой резистор. Технология нанесения таких покрытий хорошо отработана и широко применяется в современной электронной аппаратуре. Компактные высокоомные резисторы на напряжение 50 – 100 кВ также не являются дефицитом и выпускаются многими компаниями, например, Caddock Electronics, Arcol, Ohmite, Welwyn Components и др.

По нашему мнению, предлагаемое техническое решение позволит обеспечить высокий уровень помехоустойчивости МУРЗ и в реально существующих сегодня естественных условиях эксплуатации, и в экстремальных условиях при воздействии ЭМИ ЯВ или других технических средств деструктивного дистанционного элек-

тромагнитного воздействия [4.2]. При этом затраты на реализацию предложенного технического решения не будут какими-то неподъемными для электроэнергетики. Они могут быть даже существенно меньше, чем затраты на реконструкцию старой системы заземления на многих объектах электроэнергетики, не обеспечивающей нормальное функционирование МУРЗ в существующих условиях эксплуатации.

4.3. Фильтры ЭМИ ЯВ

Основными методами защиты от воздействия ЭМИ ЯВ на высокочувствительную аппаратуру являются тщательное электромагнитное экранирование самой аппаратуры и подключенных к ней внешних кабелей, а также подавление импульса посредством специальных фильтров.

4.3.1. Ферритовые фильтры

Простейшим типом фильтра, не требующим больших затрат, но, тем не менее, существенно ослабляющим воздействие короткого (то есть аналогичного по свойствам высокочастотному сигналу) электромагнитного импульса в проводах, подключенных к электронной аппаратуре, является ферритовый фильтр в форме кольца (цилиндра), одеваемого на провод, рис. 4.9.

Рис. 4.9. Ферритовые элементы (ФЭ) фильтров

Импеданс катушки, образованной одним или несколькими витками контрольного кабеля, пропущенного через ферритовое кольцо, очень мал для низкочастотных рабочих сигналов и для переменного тока промышленной частоты и очень велик для высокочастотных

(импульсных) сигналов в определенном диапазоне частот, зависящем от количества витков, материала и геометрических размеров кольца. В результате, импульсные и высокочастотные помехи, попавшие в такой кабель, будут существенно ослаблены. Затухание, вносимое такими фильтрами, составляет 10-15 дБ.

Рис. 4. 10. Миниатюрные фильтры на основе ферритовых элементов (ФЭ), предназначенные для монтажа на печатной плате

Многочисленными компаниями производится множество типов таких фильтров, как, миниатюрных, предназначенных для монтажа внутри аппаратуры на печатных платах, рис. 4.10, так и для монтажа непосредственно на проводах (кабелях). Для удобства монтажа такие фильтры часто выполняют в виде двух сопрягаемых полуколец (полуцилиндров) размещенных в защелкивающихся пластмассовых корпусах, обеспечивающих быстрый и удобный монтаж фильтров на проводах, рис. 4.11.

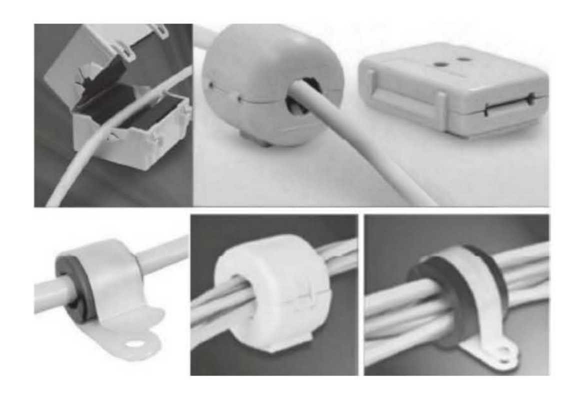


Рис. 4.11. Конструкция ферритовых фильтров для быстрого и удобного монтажа на проводах

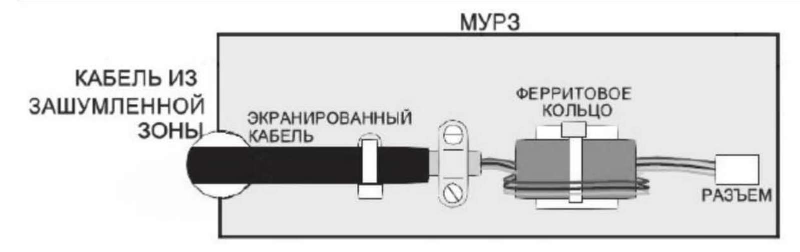


Рис. 4.12. Установка фильтра на основе ферритового кольца на контрольном кабеле, входящем в МУРЗ

В релейной защите такие фильтры можно использовать повсеместно: и в цепях питания, и в цепях передачи логических сигналов, и во вторичных цепях трансформаторов тока и напряжения, рис. 4.12.

Фильтры на основе ФЭ выпускаются многочисленными компаниями, табл. 4.1.

Табл. 4.1. Частотные характеристики фильтров на основе ФЭ, выпускаемых различными компаниями

Название компании	Частотный диапазон выпускаемых фильтров, МГц
Fire-Rite Products Corp.	1 – 1000
Ferrishield	30 – 2450
Ferroxcube	0.2 – 200
Murata	миниатюрные для печатных плат
NEC/Tokin	0.1 – 300
Parker Chomerics	30 – 200
Laird	30 – 2000
TDK	10 –500
Leader Tech, Inc	1 – 2450
Wurth Elektronik	миниатюрные для печатных плат

Приведенные в табл. 4.1. частотные диапазоны относятся не к какому-то конкретному типу фильтра, а указывают лишь область частот, в пределах которых работает та или иная компания. Частотные диапазоны конкретных типов фильтров в действительности

намного уже, указанных в табл. 4.1 диапазонов. В качестве примера на рис. 4.13 указаны частотные диапазоны материалов различных типов, используемых для производства ФЭ в компании Fire-Rite Products Corp.

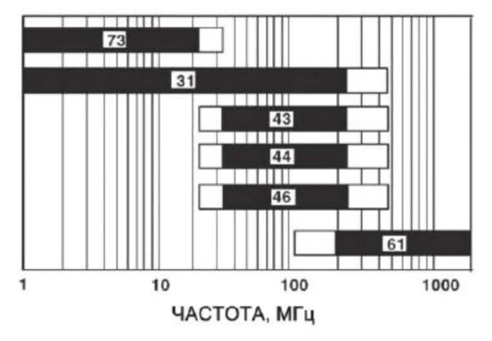


Рис. 4.13. Частотные диапазоны различных типов материалов (обозначены номерами), используемые в производстве ФЭ в компании Fire-Rite Products Corp.

Несмотря на свою кажущуюся простоту и невысокую стоимость (1 – 10 долларов США), ферритовые фильтры не так просты, как это может показаться. Их эффективность зависит от очень многих параметров: типа материала, эквивалентной частоты импульса тока, который нужно ослабить, геометрических размеров ферритового элемента (ФЭ), количества витков провода, пропущенного через него, величины постоянной составляющей тока, протекающего в проводе, температуры и др.

Частотные свойства фильтра зависят от нескольких параметров, в первую очередь от типа материала ФЭ. Для частотного диапазона от 0.1 до 2 МГц используется, как правило, марганец-цинковые ферриты (Mn-Zn) с магнитной проницаемостью $\mu = 600 - 20.000$, а для диапазона 1МГц – 2.45 ГГц – никель цинковые ферриты (Ni – Zn) с магнитной проницаемостью $\mu = 15 - 2000$. В процессе производства используются также различные смеси ферритов.

Помимо частотных характеристик, важнейшим параметром фильтра на основе ФЭ является его полное сопротивление, которым и определяется степень подавления помехи.

Полное сопротивления фильтра на основе ФЭ в значительной степени также определяется типом используемого материала, а также рабочей частотой, рис. 4.14.

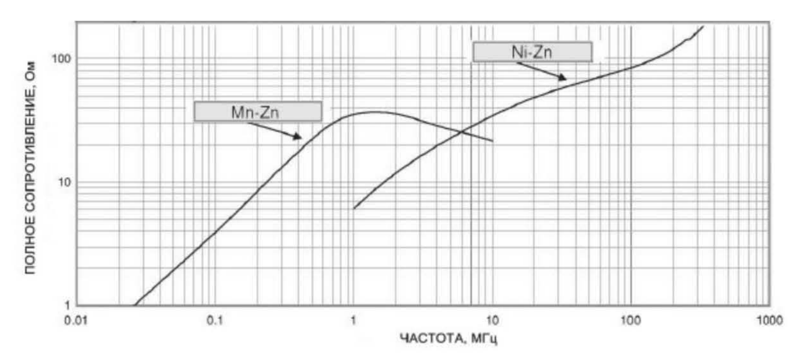


Рис. 4.14. Зависимость полного сопротивления фильтра на основе ФЭ от типа материала и частоты

Поскольку фильтры на основе ФЭ обладают индуктивностью, емкостью и активным сопротивлением, рис. 4.15, то оказывается, что частотные характеристики и полное сопротивление фильтра зависят также и от геометрических размеров ФЭ, в частности от его длины, рис. 4.16.

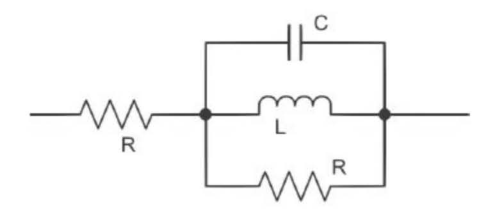


Рис. 4.15. Схема замещения фильтра на основе ФЭ

Как можно видеть из рис. 4.16, фильтры на основе ФЭ большей длины всегда обладают и большим полным сопротивлениям при остальных равных параметрах, что объясняется большим индуктивным сопротивлением фильтров с длинными ФЭ.

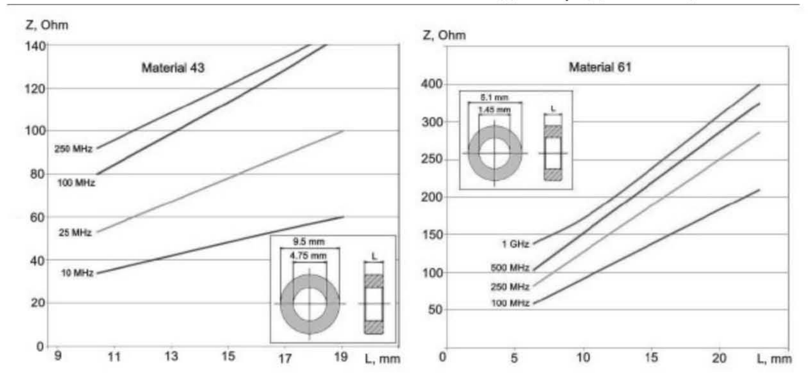


Рис. 4.16. Зависимость полного сопротивления Z фильтра от длины L ферритовых элементов, выполненных из материалов двух типов (43 и 61) компании Fire-Rite Products Corp.

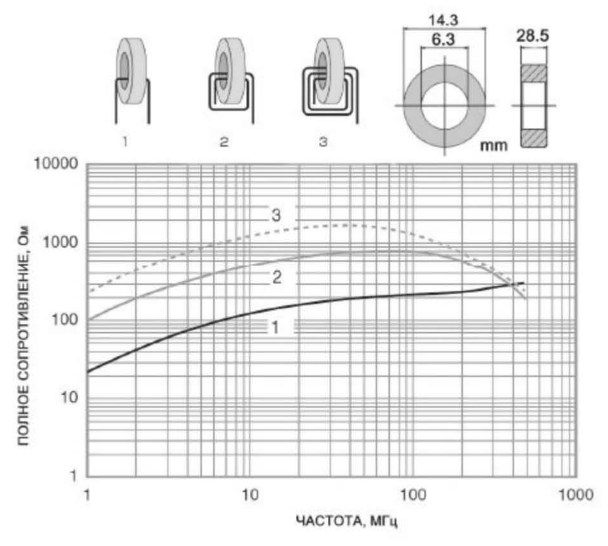


Рис. 4.17. Типичная зависимость полного сопротивления фильтра от количества витков (обозначены цифрами 1 – 3), пропущенных через ФЭ

Полное сопротивление фильтров на основе ФЭ в значительной степени зависит также и от количества витков провода, пропущенного через ФЭ, рис. 4.17. Как можно видеть из рис. 4.17, с ростом частоты помехи полное сопротивление фильтра с несколькими витками провода начинает снижаться значительно быстрее, чем фильтра с одним витком, что можно объяснить большей емкостью фильтра с несколькими витками. При дальнейшем увеличении частоты помехи фильтры с несколькими витками провода оказываются уже менее эффективными, чем фильтры с одним витком.

Еще одно, довольно неприятное свойство фильтра на основе ФЭ, заключается в наличии зависимости его свойств от величины постоянной составляющей тока, протекающего через него, рис. 4.18. Это влияние обусловлено изменением магнитных свойств ФЭ при наличии постоянной составляющей в токе.

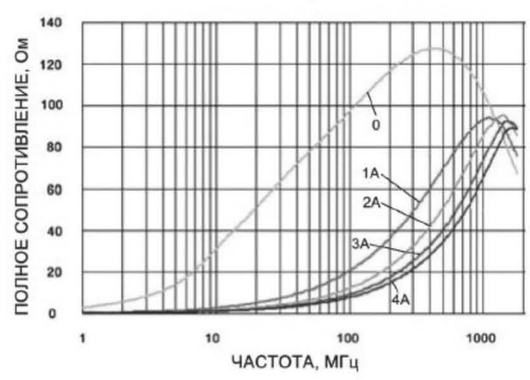


Рис. 4.18. Влияние постоянной составляющей в токе фильтра на его характеристики

Наличие индуктивности и емкости в схеме замещения фильтра (рис. 4.15) обуславливает опасность возникновения резонанса при определенных частотах, когда вместо ослабления сигнала помехи произойдет ее усиление – что является еще одним неприятным свойством такого фильтра.

Как же правильно выбрать фильтр для эффективной защиты от ЭМИ ЯВ при наличии такого большого количества факторов, влияющих на его параметры? Непросто. Особенно, если учесть отсутствие стандартов, описывающих процедуру измерения параметров

таких фильтров и использование различными производителями различных методик для таких измерений, что делает практически несопоставимыми параметры фильтров, изготовленных различными производителями.

На основе проведенного выше анализа, можно рекомендовать следующие основные принципы правильного выбора фильтров с ФЭ:

1. Для эффективного подавления импульсной помехи в максимально широком диапазоне частот ПЭДВ необходимо использование, по крайней мере, трех последовательно установленных на одном проводе (кабеле) фильтров, выполненных из различных материалов, обеспечивающих максимальные значения полного сопротивления фильтров, лежащие в области низких частот (0.1 МГц), средних частот (300 – 500 МГц) и высоких частот (2 – 2.45 ГГц). Использование трех последовательно установленных на одном проводе фильтров решает также проблему резонанса, поскольку у трех фильтров с различными характеристиками будут и существенно отличающиеся резонансные частоты.
2. Данные производителей могут быть использованы лишь для предварительного отбора фильтров, после которого должно быть проведено испытание эффективности подавления помехи выбранными фильтрами во всем интересующем потребителя диапазоне частот и токов.

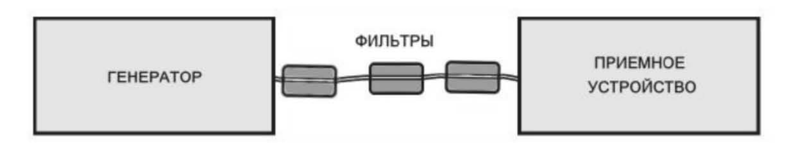


Рис. 4.19. Установка для проверки эффективности фильтров на основе ФЭ

Такое испытание может быть реализовано на установке, содержащей генератор помехи с реальными параметрами (по меньшей мере с реальным частотным диапазоном) и приемное устройство, в качестве которого может служить осциллограф, анализатор спектра и даже электронный вольтметр с расширенным частотным диапазо-

ном. Генератор соединяется с входом приемного устройства с помощью кабеля с установленными на нем фильтрами, рис. 4.19.

4.3.2. Фильтры на основе LC-звеньев

Многочисленными компаниями выпускаются также специальные фильтры на основе LC-звеньев, рис. 4.20, через которые осуществляется связь защищаемой электронной аппаратуры с внешними устройствами и системами.

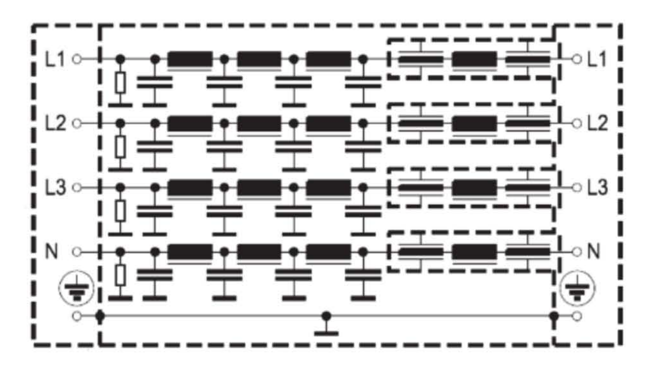


Рис. 4.20. Типовая схема силового фильтра ЭМИ ЯВ, состоящая из набора LC звеньев

Современный рынок таких фильтров представлен сегодня десятками типов, производимых многочисленными компаниями: ETS-Lindgren, MPE, Meteolabor-EMP, European EMC Products Ltd., Captor Corp., LCR Electronics, API Technologies, Astrodyne TDI Corp., Fi-Coil, EMI Solutions Pvt. Ltd, RFI Corp., и др. Казалось бы, в чем проблема: хочешь защитить свою аппаратуру от ЭМИ ЯВ? Установи такие фильтры и спи спокойно! Но вот вопрос, действительно ли можно спать спокойно, после установки таких фильтров?

При попытке выбрать фильтр, способный эффективно подавлять ЭМИ ЯВ, неожиданно сталкиваешься с проблемой: все перечисленные выше компании рекламируют свои фильтры, как высокоэффективные средства защиты от ЭМИ ЯВ и при этом ссылаются на соответствие этих фильтров военному стандарту MIL-STD-188-125 [4.6], однако при этом они указывают параметры испытатель-

ных импульсов, которым были подвергнуты фильтры, существенно отличающихся от указанных в стандарте. Так, например, этот стандарт предусматривает испытания импульсами тока 20/500 нс определенной амплитуды, на нагрузку 60 Ом, тогда как фильтры испытываются производителями импульсами тока 8/20 мкс на нагрузку 1 Ом. Почему? Да потому, что импульс 8/20 мкс – это стандартный импульс, воспроизводимый всеми видами испытательной аппаратуры, предназначенной для испытания на устойчивость к разряду молнии, тогда как для испытания импульсами тока 20/500 нс на нагрузку 60 Ом требуется специальная весьма дорогостоящая аппаратура, которой нет у производителей фильтров. Об этой проблеме прямо говорится в [4.7].

Еще одна странность заключается в том, что MIL-STD-188-125 предусматривает испытания объекта импульсами тока в двух режимах: при протекании тока между всеми объединенными вместе входами и землей (common mode) и между каждым входом отдельно и землей (wire-to-ground mode).

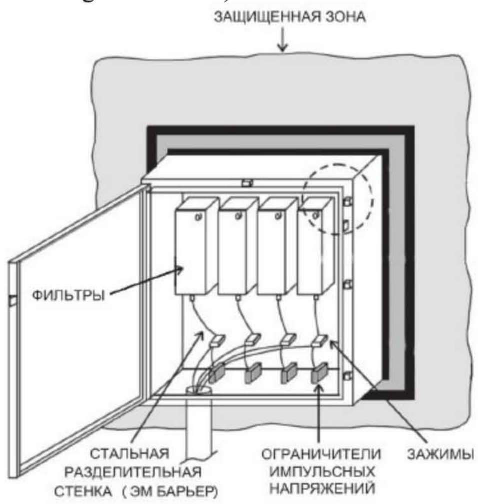


Рис. 4.21. Устройство вводной коробки для подключения внешнего кабеля к защищенному от ЭМИ ЯВ объекту (по версии MIL-STD-188-125)

Однако, при высотном ядерном взрыве импульс высокого напряжения может прикладываться не только между входами аппаратуры и землей (этот режим в других стандартах обозначен как «common mode»), но и между различными входами изолированной от земли аппаратуры («differential mode»).

Стандарт MIL-STD-188-125 не предусматривает таких испытаний, они рассматриваются в других стандартах. В связи с этим, некоторые компании, рекламирующие свои фильтры, как фильтры ЭМИ ЯВ, вообще не снабжают их элементами ограничения импульсных напряжений, ссылаясь все на тот же MIL-STD-188-125, но при этом утверждают, что поскольку их фильтры прошли испытания импульсом тока с амплитудой в несколько тысяч ампер и признаны соответствующими стандарту MIL-STD-188-125, то это значит, что они обеспечивают полноценную защиту от ЭМИ ЯВ. Действительно, в этом стандарте ограничители импульсных напряжений представлены как совершенно самостоятельные элементы, не имеющие отношения к фильтрам, рис. 4.21.

При таком подходе, фильтры действительно не обязаны защищать от перенапряжений на входах. Вот только можно ли при таком подходе утверждать, что эти самые фильтры являются полноценной защитой от ЭМИ ЯВ? Очевидно, понимая проблему, многие производители все же снабжают свои фильтры элементами защиты от импульсных перенапряжений, установленными на входах. По их мнению, теперь такие фильтры с полным правом можно называть фильтрами защиты от ЭМИ ЯВ.

Однако, при внимательном рассмотрении защитных элементов, применяемых в этих фильтрах, возникают серьезные сомнения в их эффективности. Наиболее распространенные и дешевые ограничители импульсных напряжений, применяемые в фильтрах, это газовые разрядники и оксидно-цинковые варисторы, рис. 4.22. Как известно, они являются относительно «медленными» элементами, хорошо справляющимися с подавлением стандартных импульсов 8/20 мкс, но не успевающими сработать при воздействии короткого импульса высокого напряжения Е1 ЭМИ ЯВ с параметрами 2/25 нс [4.8] (или 5/50 нс по данным [4.9]). Потребитель же, прочитав, что выбранный им фильтр предназначен для защиты от ЭМИ ЯВ и прошел испытания импульсами тока 8/20 мкс в полном соответствии с военным стандартом MIL-STD-188-125, вряд ли будет ис-

кать этот стандарт и проверять, а действительно ли это тот самый импульс.

Рис. 4.22. Фильтры компании MPE с защитными элементами на входе, в качестве которых применяются варисторы (VDR) и газовые разрядники (GDT)

Однако, предъявлять претензии производителям рано. В [4.10] прямо говорится о том, что установленные в фильтрах недостаточно быстрые варисторы и еще более медленные газовые разрядники, оказывается, вообще не предназначены для защиты от ЭМИ ЯВ, а являются элементами защиты от разрядов молнии и коммутационных перенапряжений. Вот так: в фильтрах для защиты от ЭМИ ЯВ применяются ограничители напряжения, предназначенные для защиты от ... молнии, но не от ЭМИ ЯВ! Тем не менее, некоторые типы фильтров компании MPE с защитными варисторами названы в рекламных проспектах фильтрами, специально предназначенными для защиты от компонента E1. Однако, внимательный анализ параметров этих фильтров показал, что они ничем, кроме названия в заголовке, не отличаются от всех остальных фильтров этой компании, то есть, на самом деле, защищены от разрядов молнии, а не от компонента E1 ЭМИ ЯВ. В противном случае нужно будет признать, что параметры разряда молнии ничем не отличаются от параметров компонента E1, что на самом деле совершенно не соответствует действительности.

В дискуссии с представителем компании MPE по поводу обоснованности применения варисторов в фильтрах, предназначенных для защиты от ЭМИ ЯВ, был выдвинут один новый довод. Представитель компании заявил, что несмотря на то, что варистор сам по себе не очень быстрый элемент, в соединении с L-C элементами фильтра, его эффективность становится достаточной для защиты от компонента E1. Проверка этого довода компании показала, что и он не точен. В ряде публикаций на эту тему [4.11 – 4.12] утверждается, что присоединение к защитному элементу даже коротких внешних проводников, обладающих очень малой индуктивностью, снижает его быстродействие. Оказывается, что время реакции защитного элемента на приложенный к нему импульс напряжения очень сильно зависит и от конструкции корпуса этого элемента, и от формы (длины) его выводов [4.11 – 4.12]. Более того, в [4.12] утверждается, что именно конструкция и длина внешних выводов определяет время реакции защитного элемента. Зная это, производители защитных элементов часто указывают в рекламных материалах время реакции не полностью собранного элемента в корпусе с выводами, а лишь материала, используемого для изготовления этого защитного элемента [4.12]. Вместе с тем, производители работают над усовершенствованием конструкции выводов защитных элементов и добиваются существенных успехов [4.13].

Из изложенного выше становится понятным, что получить объективные данные о быстродействии того или иного типа защитного элемента можно только проведя собственные независимые испытания готовых изделий, предлагаемых на рынке, хотя некоторые косвенные данные о результатах таких испытаний [4.14], позволяют произвести предварительную сравнительную оценку. Так, например, по утверждению [4.14], динамическое сопротивление и время реакции защитного элемента на основе лавинного диода (TVS diode) почти в 10 раз меньше, чем варистора. Мы не проводили собственных исследований быстродействия этих диодов и варисторов для того, чтобы подтвердить или опровергнуть эти данные, однако, тот факт, что для защиты электронной от аппаратуры от высоковольтных электростатических разрядов (а это наносекундный диапазон, то есть наиболее близкий по временному параметру к ЭМИ ЯВ) применяются защитные элементы на основе лавинных диодов, а не варисторов, говорит сам за себя.

Наиболее мощные TVS-диоды (импульсный ток до 10 кА, остающееся напряжение 200 – 500 В) производятся компанией Bourns, Inc. Такими ограничителями импульсных напряжений снабжены фильтры компании Captor Corp., рис. 4.23, которые и рекомендуется использовать в электроэнергеткие.

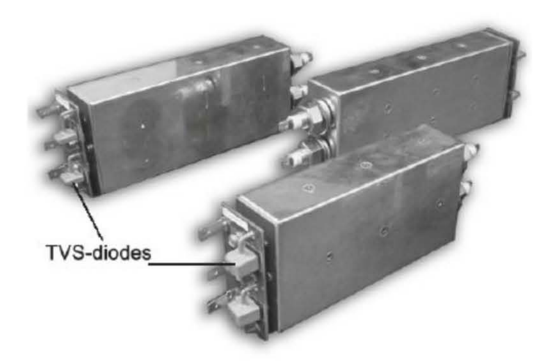


Рис. 4.23. Фильтры ЭМИ ЯВ компании Captor Corp., снабженные мощными быстродействующими ограничителями амплитуды импульсных напряжений на базе TVS-диодов

Еще одной проблемой, связанной с использованием элементов защиты от импульсных напряжений, является схема включения этих элементов, принятая в большинстве фильтров, рис. 4.20, при которой каждый такой элемент включен между входом и заземленным корпусом фильтра. При таком включении получается, что между входами фильтра оказываются включенными два последовательно соединенных элемента, обуславливающих двойное остаточное напряжение, которое может представлять опасность для защищаемой электронной цепи.

Технические требования по устойчивости аппаратуры к таким напряжениям и методы ее испытаний описаны в стандартах IEC 61000-4-4 [4.9] и IEC 61000-4-25[4.15]. Под испытательным импульсом такого напряжения подразумевается так называемый Electrical Fast Transient (EFT) – быстрый импульс, параметры которого и методика испытаний описаны в стандарте IEC 61000-4-4, рис. 4.24. Методика выбора параметров испытательных импульсов

на основе этих стандартов для конкретного примера – микропроцессорного устройства релейной защиты (МУРЗ), изложена в [4.16], для которого амплитуда импульсного напряжения EFT составила 8 кВ.

По нашему мнению, таким испытаниям должны подвергаться фильтры с элементами защиты от импульсных напряжений, предназначенные для защиты от ЭМИ ЯВ в дополнение к испытаниям, предусмотренным стандартом MIL-STD-188-125, причем, с приложением испытательных напряжений как между входами и землей, так и между отдельными входами.

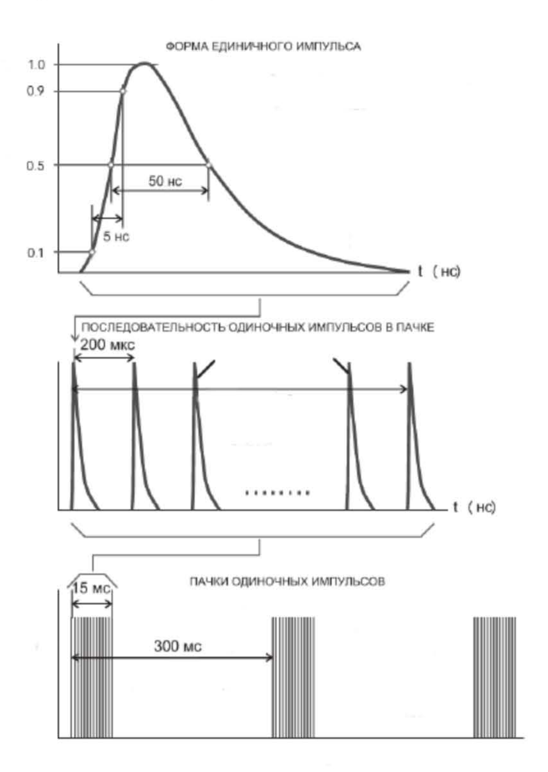


Рис. 4.24. Electrical Fast Transient (EFT) – быстрый импульс (IEC 61000-4-4)

Еще одна проблема связана с амплитудно-частотной характеристикой фильтров. Типовая характеристика высококачественного фильтра, предназначенного для защиты от ЭМИ ЯВ, приведена на рис. 4.25. Как же параметры реальных фильтров связаны с этой типовой характеристикой?

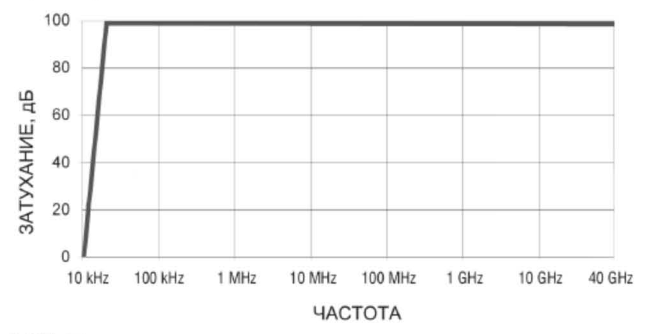


Рис. 4.25. Типовая амплитудно-частотная характеристика высококачественных фильтров ЭМИ ЯВ

Одни компании (как, например, Meteolabor) вообще не приводят в техническом описании некоторых своих фильтров данные о частотном диапазоне и вносимом затухании. Другие (например, MPE) приводят в своей документации типовую характеристику, которой должны обладать фильтры в соответствии со стандартом MIL-STD-188-125 (частотный диапазон 14 кГц – 40 ГГц, затухание во всем диапазоне 100 дБ) и тут же приводят реальные характеристики производимых фильтров с параметрами: 10 кГц – 1 ГГц с затуханием 80 дБ – для фильтра обычного качества и тот же частотный диапазон, но с затуханием 100 дБ – для фильтра улучшенного качества. А куда же подевался частотный диапазон от 1 ГГц до 40 ГГц? Сотрудники компании Astrodyne (LCR Electronics, Inc.) оказались хитрее. Они написали в технической документации на свои фильтры, что они обеспечивают затухание в 100 дБ в частотном диапазоне 14 кГц – 10 ГГц в соответствии со стандартом MIL-STD-220 [4.17], но если их фильтры будут хорошо экранированы и изолированы (читай: установлены в «клетке Фарадея»), то их частотный диапазон может быть расширен до требуемого значения 40 ГГц. Вот так: чтобы фильтр «правильно» защищал от ЭМИ ЯВ, его самого сначала

нужно защитить от этого самого ЭМИ ЯВ! Как говорится, комментарии излишни.

Табл. 4.2. Частотные характеристики фильтров ведущих производителей

Производитель фильтров ЭМИ ЯВ	**Частотный интервал**		**Затухание, дБ**	**Примечание**
	Min	**Max**		
LCR Electronics	14 kHz	1 GHz	100	-
MPE	10 kHz	1 GHz	80	для стандартного фильтра
MPE	14 kHz	18 GHz	100	для улучшенного фильтра
Fi-Coil	14 kHz	1 GHz	100	-
Captor Corp.	14 kHz	10 GHz	100	-
ETS-Lindgren	14 kHz	40 GHz	100	-
MeteoLabor	200 kHz	1 GHz	80	для фильтра типа PLP
MeteoLabor	-	-	-	для фильтра типа USP

Вся комичность ситуации отражена в табл. 4.2 , в которой приведены для сравнения частотные характеристики фильтров ведущих производителей: все фильтры имеют одно и то же назначение и все соответствуют требованиям стандарта MIL-STD-188-125, и при этом все они имеют существенно различающиеся параметры. Как же такое может быть?

Еще одной особенностью принятой схемы включения отдельных внутренних элементов фильтров между каждым входом и землей, является не только двойное остаточное напряжение на элементах защиты от импульсных напряжений, о чем упоминалось выше, но и двойная емкость и двойная индуктивность, включенная между входами по сравнению с индуктивностью и емкостью между каждым входом и землей. Отсюда следует, что частотные характеристики фильтров для импульса, приложенного между входами, будут не такими, как для импульса, приложенного между входом и землей. Насколько эти характеристики будут приемлемы для защиты от ЭМИ ЯВ?

И какой потребитель будет так глубоко «копать»? Почему он не должен поверить утверждениям компании-производителя о высокой эффективности ее продукции? А если даже и не поверит, то все равно не сможет, в большинстве случаев, самостоятельно проверить реальную эффективность «работы» такого фильтра. Понятно, какова будет эффективность защиты его ответственной аппаратуры фильтром, если в критической ситуации он окажется не способным защитить от ЭМИ ЯВ.

Сегодня ситуация такова, что каждый производитель сам решает, включать или не включать ограничители импульсного напряжения в состав фильтров; использовать или не использовать дешевые, но не подходящие по своим параметрам элементы; испытывать фильтры стандартным «грозовым» импульсом, или импульсом с параметрами, оговоренными в военном стандарте, упоминать или вообще не упоминать о частотном диапазоне, использовать частотный диапазон, оговоренный в стандарте MIL-STD-188-125 или в стандарте MIL-STD-220 [4.17], а может быть и указать собственный частотный диапазон и при этом дать ссылку на известный военный стандарт. Кто там будет проверять!

Сложившееся положение дел - следствие отсутствия специального стандарта, оговаривающего требования к конструкции и к параметрам фильтров ЭМИ ЯВ, методам их испытаний, критериям качества функционирования. Такая ситуация является, по нашему мнению, недопустимой, учитывая важность проблемы, и требует незамедлительного исправления.

4.4. Нелинейные ограничители перенапряжений

Эффективной мерой борьбы с наведенными перенапряжениями на входах электронной аппаратуры и на ее зажимах питания является широкое использование элементов с нелинейной характеристикой: газовых разрядников, варисторов, специальных полупроводниковых элементов на основе стабилитронов, и т.д. включаемых параллельно защищаемому объекту (например, параллельно входу МУРЗ) и между каждой клеммой этого объекта и землей. Элементами, обладающими наилучшими характеристиками, считаются на сегодняшний день резисторы с нелинейной характеристикой, выполненные из прессованного порошка оксида цинка ZnO (реже из

карбида кремния, титаната бария и др. материалов) – варисторы, которые и получили наибольшее распространение. Выпускаются они сегодня в огромных количествах: без корпусов, в корпусах различных типов, часто снабжаются всякими вспомогательными элементами (предохранителями, сигнальными флажками и т.п.). Варисторы должны быть правильно выбраны. К сожалению, часто приходится наблюдать, ситуацию, при которой варисторы даже в аппаратуре ведущих мировых производителей выбраны неверно и, фактически, никакими защитными функциями не обладают.

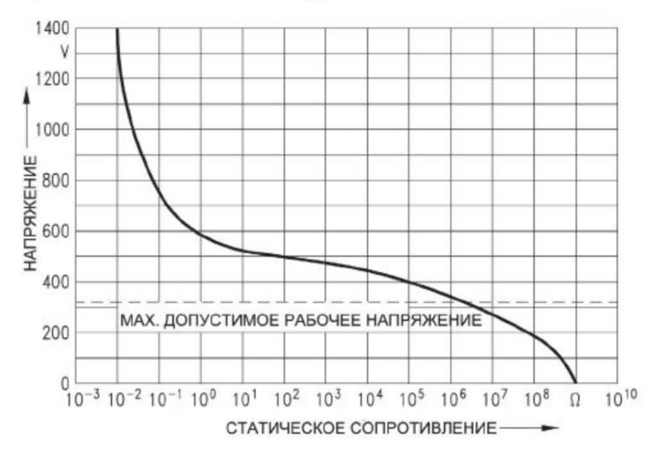


Рис. 4.26. Типовая ВАХ оксидноцинкового варистора

Поскольку вольтамперная характеристика (ВАХ) варистора далеко не идеальна, рис. 4.26, правильно выбрать его не так-то просто. С одной стороны, варистор не должен пропускать через себя ток более 1 мА (стандартное значение для современных варисторов) при максимальном рабочем напряжении (иначе он просто перегреется и сгорит), с другой - остаточное напряжение на нем после срабатывания (clamping voltage) должно быть заметно меньше напряжения, выдерживаемого электронными компонентами защищаемого оборудования (в противном случае не варистор будет защищать электронные компоненты, а эти компоненты будут «защищать» варистор).

Из-за несовершенства ВАХ варисторов для выполнения этих условий максимальное выдерживаемое напряжение электронных компонентов, предназначенных для работы в сети 220 В, должно быть не менее 1000 В. Однако, во первых, электронные компоненты на такое напряжение значительно дороже, чем низковольтные, во-вторых, они обладают худшими другими характеристиками. Например, транзисторы на напряжение 1000 – 1200 В имеют значительно меньший коэффициент усиления и значительно большее падение напряжения в открытом состоянии, чем такие же транзисторы на напряжение 400 – 500 В. Поэтому довольно часто приходится встречать, например, в источниках питания МУРЗ, регистраторов аварийных режимов и в другой электронной аппаратуре ведущих мировых производителей транзисторы с максимальным выдерживаемым напряжением 500 В, работающие непосредственно в цепи 220 – 250 В. Обеспечить защиту электронных компонентов варисторами при таком соотношении рабочего и максимально выдерживаемого напряжения просто невозможно.

Рис. 4.27. Мощные варисторы различных типов с номинальным напряжением 130 – 1100 В и разрядным током от 3 - 100 кА

Современные металлооксидные варисторы обладают большой мощностью, рис. 4.27 и выпускаются в пластмассовых корпусах,

специально предназначенных для установки на стандартную DIN-рейку в монтажных шкафах, рис. 4.28.

Рис. 4.28. Защитные устройства большой мощности на основе металлооксидных варисторов компании Square D (Schneider Electric), предназначенные для установки на стандартную DIN-рейку

К сожалению, такие замечательные элементы имеют недостаточно высокое быстродействие (для целей защиты от ЭМИ ЯВ). Их характеристики ухудшаются (деградируют) при неоднократном воздействии мощных импульсных нагрузок.

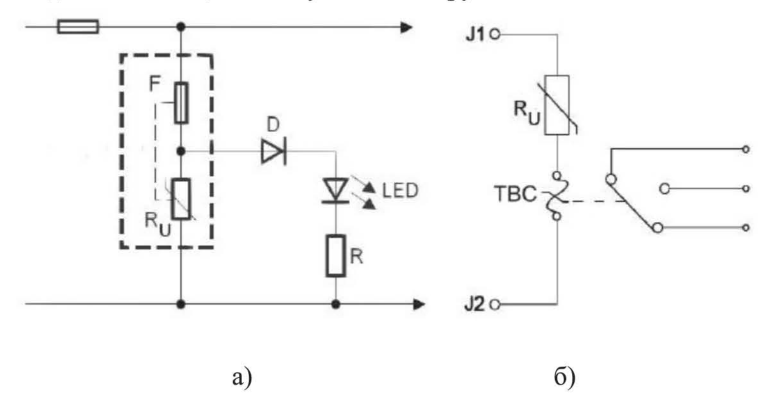


Рис. 4.29. Схемы включения варисторов с предохранителем F (а) и с термобиметаллическим контактом ТВС (б)

При этом возрастает ток утечки через варистор при нормальном напряжении, он начинает перегреваться, при этом его сопротивление уменьшается, а ток еще больше возрастает, вплоть до сгорания. Иногда это заканчивается коротким замыканием в питающей сети со всеми вытекающими отсюда последствиями. Поэтому в последнее время на рынке появились варисторы со встроенными предохранителями, соединенными последовательно с варистором. При резком возрастании тока через варистор, предохранитель сгорает и включает сигнальный светодиод, рис. 4.29а. Иногда вместо обычного предохранителя используется термобиметаллический контакт, расположенный на варисторе и срабатывающий при увеличении температуры варистора, рис. 4.29б. Контакт можно включить в цепь сигнализации, оповещающей персонал о необходимости заменить варистор.

Для защиты сетей постоянного тока, а на подстанциях и электростанциях это разветвленные и протяженные сети цепей оперативного питания, применяются специальные защитные устройства на варисторах.

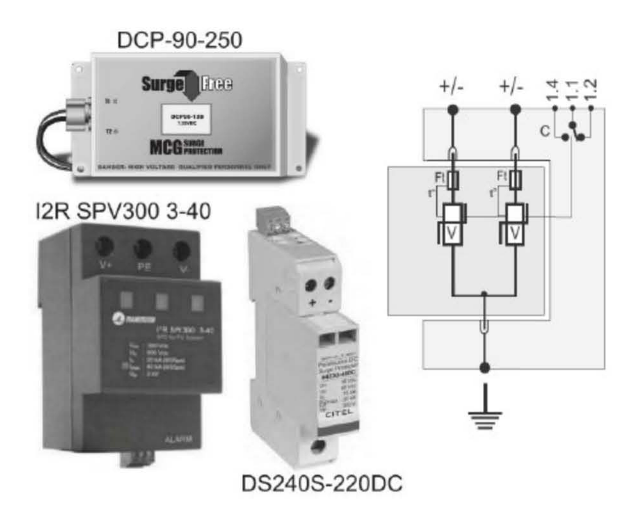


Рис. 4.30. Защитные устройства на варисторах для сетей постоянного тока с номинальным напряжением 220 В

Эти устройства содержат, как правило, два или три варистора, снабженные термобиметаллическим контактом, обеспечивающими защиту от перенапряжений между «+» и «-», между «+» и «землей», между «-» и «землей», рис. 4.30. Эти устройства обеспечивают протекание разрядного тока в пределах 40 – 200 кА и более.

Отмеченный выше недостаток варисторов – недостаточное для защиты от короткого импульса ЭМИ ЯВ быстродействие отсутствует у высокоскоростных кремниевых ограничителей перенапряжений, выполненных на базе зенеровских диодов (Transient Voltage Suppressor Diodes или TVS Diodes), действие которых основано на резком лавинообразном изменении сопротивления от относительно высокого значения практически до нуля при превышении приложенного к ним напряжения определенной пороговой величины, рис. 4.31.

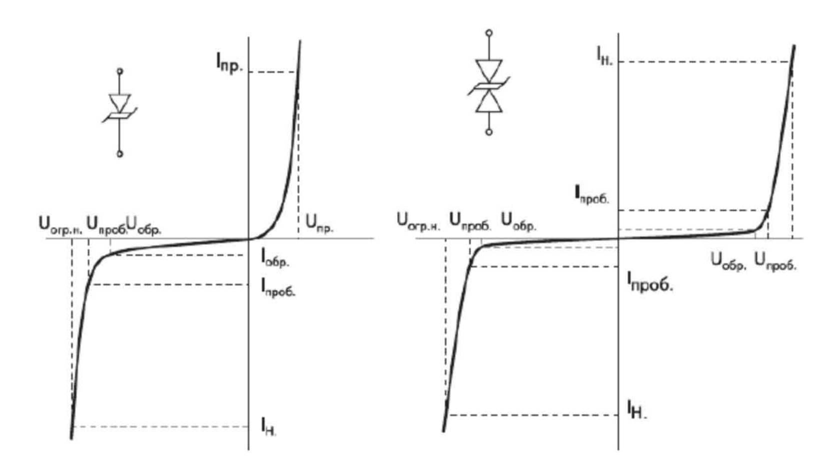


Рис. 4.31. Вольтамперные характеристики однонаправленных (для постоянного тока) и двунаправленных (для переменного тока) диодных супрессоров

Кроме того в отличие от варисторов характеристики таких ограничителей перенапряжений на базе TVS-диодов, после многократных воздействий высоких напряжений и переключений режимов не ухудшаются. До недавнего времени такие защитные эле-

менты обладали недостаточной импульсной рассеиваемой мощностью и поэтому использовались лишь в маломощных цепях электронной аппаратуры. Однако, в последнее время на рынке появились и мощные супрессоры, рис. 4.32. Так, например, широко известной компанией Littelfuse, специализирующейся на разработке и производстве элементов защиты от перенапряжений был налажен выпуск супрессоров с импульсной мощностью до 30 кВт, допускающих протекание разрядных импульсных токов до нескольких сотен ампер. TVS-диоды компании UN Semiconductor способны пропускать импульсы тока с амплитудой до 3 кА и работать при напряжениях до 440 В. Наиболее мощные TVS-диоды (импульсный ток до 10 кА, остающееся напряжение 200 – 500 В) производятся компанией Bourns, Inc.

Рис. 4.32. Мощные быстродействующие ограничители амплитуды импульсных напряжений на основе лавинных диодов

Диодные супрессоры, как и варисторы можно соединять параллельно для увеличения разрядного тока.

Для повышения эффективности защиты от перенапряжений можно использовать также параллельное соединение разнотипных ограничителей перенапряжения, например таких, как варисторы и полупроводниковые супрессоры, рис. 4.33. Такое гибридное устройство обладает прекрасными характеристиками.

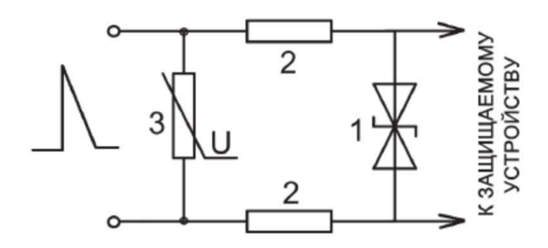


Рис. 4.33. Гибридное защитное устройство: 1 – полупроводниковый супрессор; 2 – токоограничивающие резисторы; 3 – мощный варистор

Первым в нем всегда срабатывает быстродействующий супрессор 1, реагирующий на импульс даже с очень крутым передним фронтом и поглощающий часть его энергии. Разрядный ток ограничивается резисторами 2, что предотвращает разрушение супрессора. Падение напряжения на резисторах 2 повышает напряжение на варисторе 3, что приводит к резкому уменьшению его сопротивления и шунтированию резисторов. Оставшаяся (большая) часть энергии поглощается мощным варистором.

При установке мощных варисторов на шинах систем постоянного и переменного тока, а менее мощных TVS-диодов в непосредственной вблизи от входов защищаемых электронных приборов получается высокоэффективная система защиты.

4.5. Экранирование контрольных кабелей

Основным средством защиты контрольных кабелей от наведенных напряжений является их экранирование, а также выбор правильного способа прокладки с учетом максимально возможного удаления от молниеотводов и от силовых кабелей, использование специальных кабельных лотков. Существует несколько типов таких лотков: пластмассовых со вставками из алюминия, пластмассовых с напылением металла, алюминиевых.

В общем случае эффективность металлического экрана (то есть степень ослабления электромагнитного поля) обусловлена двумя

его свойствами: поглощением энергии при прохождении электромагнитной волны через проводящую среду и отражением волны на границе раздела двух сред. Оба эти явления зависят как от частоты электромагнитной волны, так и от материала экрана. Лучшее поглощение электромагнитной энергии обеспечивают ферромагнитные материалы (железо, пермендюр, пермаллой), а лучшее отражение электромагнитной волны обеспечивается диамагнитными материалами (медь, алюминий). Эффективность экранирующих свойств ферромагнитных материалов снижается с увеличением напряженности поля из-за насыщения, а эффективность диамагнитных экранов снижается с ростом частоты из-за роста сопротивления. По ряду причин технического и экономического порядка наибольшее распространение получили экраны в виде медной сетки (оплетки) и различных профилей из алюминия.

Поскольку глубина проникновения электромагнитной волны в металл зависит обратно пропорционально от частоты этой волны, то очевидно, что чем толще экранирующая металлическая оболочка, тем для более широкого частотного диапазона она будет эффективно ослаблять электромагнитное поле. Например, если для эффективного экранирования на частоте 500 кГц достаточной является толщина медного экрана около 0.6 мм, то для промышленной частоты 50 Гц необходим медный экран с толщиной стенок уже около 6 см (для ферромагнитного экран достаточна стенка в 5 мм).

Исходя из изложенного, очевидно, что наименьшим экранирующим эффектом обладают пластмассовые лотки с металлическим напылением, широко используемые для прокладки контрольных кабелей. Такая конструкция начинает работать эффективно лишь на частотах 600 МГц и выше. На частотах ниже 200 МГц она вообще не работает. Наводки на контрольные кабели на подстанциях имеют, обычно, значительно более низкую частоту, чем указанные 200 МГц, поэтому применение пластмассовых лотков с напылением вообще бессмысленно. Вместе с тем, алюминиевые лотки и медная оплетка на кабелях все еще способны ослабить наводимые напряжения в десятки раз и поэтому они нашли широкое применение. Наибольшее ослабление наводок в широком диапазоне частот может обеспечить прокладка контрольных кабелей в стальных водопроводных трубах.

Для успешного функционирования экранных оболочек необходимо обеспечить стекание наведенного на них заряда в землю. В идеальном случае потенциал по всей длине экрана должен быть равным потенциалу земли, поэтому иногда в особо чувствительных высокочастотных электронных цепях применяют многократное заземление экрана кабеля через каждые 0.2λ (λ - длина волны электромагнитного поля).

При прокладке экранированных кабелей на подстанциях может использоваться такое дополнительное решение как прокладка параллельно трассе кабелей медной шины выравнивания потенциалов, заземленной с двух сторон. Однако, по экономическим соображениям чаще используется простое заземление экрана с одной или с двух сторон, рис. 4.34.

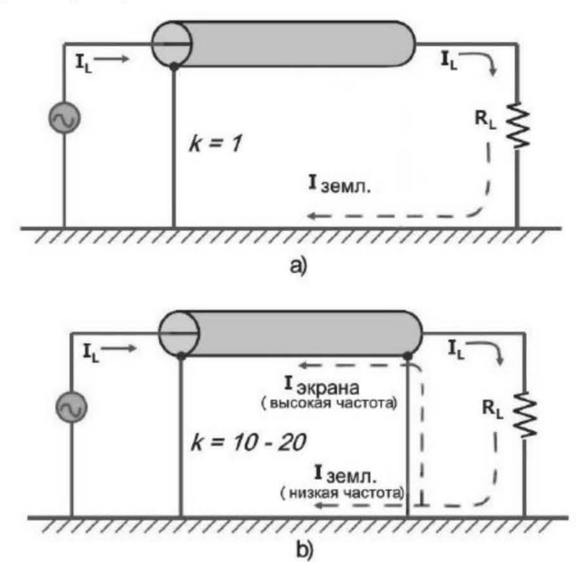


Рис. 4.34. Работа экрана, заземленного с одной и с двух сторон

Часто приходится слышать мнение релейщиков о целесообразности заземления экранов контрольных кабелей лишь с одной стороны. По-видимому, это мнение возникло под влиянием двух известных релейщикам фактов: заземления токовых цепей лишь с од-

ной стороны, а также заземления экранов силовых высоковольтных кабелей с одной стороны. Эти известные факты иногда переносятся на заземление экранов контрольных кабелей без учета того, что заземление в приведенных выше примерах является средством обеспечения электробезопасности, а не защиты от помех

В действительности, заземление экрана контрольного кабеля с одной стороны является эффективным лишь против емкостных наводок, рис. 4.35 (так называемая электростатическая защита) и совершенно не эффективной мерой (коэффициент ослабления помехи k = 1) для индуктированных наводок, поскольку этот экран не обеспечивает цепи для замыкания тока помехи.

Рис. 4.35. Импульсная наводка через емкостную связь между проводниками

При заземлении экрана с двух сторон, появляется дополнительная цепь (экран), обладающая значительно меньшим импедансом для высокочастотного сигнала, чем земля. В результате, рабочий сигнал, делится на две части, одна из которых (низкочастотная) попрежнему, возвращается через землю, а вторая (высокочастотная) – через экран кабеля. Таким образом, для высокочастотной составляющей ток в экране равен току в центральной жиле, направленному встречно, и компенсируется благодаря электромагнитной связи между экраном и центральной жилой. Так обеспечивается защита от высокочастотного излучения с центральной жилы во внешнее пространство (то есть на соседние кабели) с коэффициентом ослабления помехи k = 3 - 20. Эта система работает также эффективно и при внешнем электромагнитном воздействии на экран, при котором наведенный в экране высокочастотный сигнал замыкается через землю. При выполнении присоединения экрана к земляной шине следует иметь ввиду, что никакие «накрутки» соединительного провода на экран недоспустимы, как недопустимо

и свертывание в кольца длинного соединительного провода между экраном и земляной шиной. Каждый дополнительный виток этого провода увеличивает импеданс системы заземления на высоких частотах и резко снижает ее эффективность.

Мощным источником помех на подстанциях иногда выступают источники, совершенно не явные и не очевидные. Например, на одной из Российских подстанций были зафиксированы случаи ложных отключений одного из высоковольтных выключателей при подаче команды на отключающую катушку другого выключателя. Контрольные кабели идущие к отключающим катушкам обоих выключателей были не экранированы и проходили в общем лотке на протяжении, примерно, 25 м. Эксперименты с осциллографированием напряжений, выполненные на этой подстанции, рис. 4.36, показали, что на катушке ложно сработавшего выключателя могут наводиться импульсы с амплитудой 500 – 728 В при подаче управляющего напряжения 220 В на катушку второго выключателя.

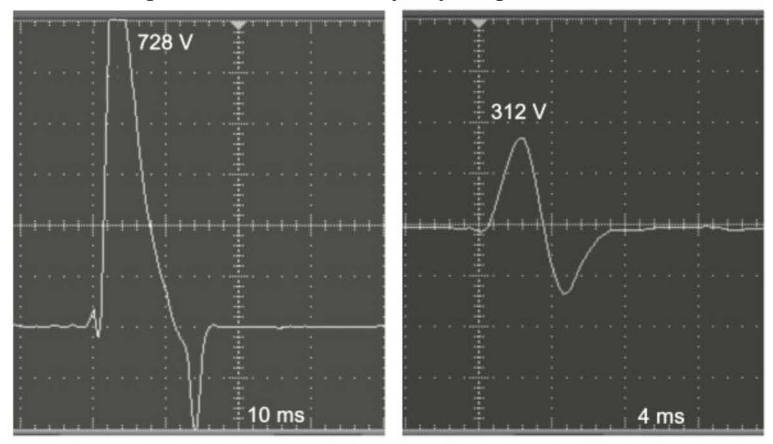


Рис. 4.36. Индуктированные наводки одного контрольного кабеля на другой: слева – не экранированные кабели; справа – один кабель экранирован с двух сторон

Длительность этого наведенного импульса иногда бывает такой, что приводит к ложному срабатыванию выключателя. Возникновение столь мощной импульсной помехи в цепях управления вызыва-

ет некоторое недоумение и даже замешательство. Все становится понятным, если вспомнить, что катушка отключения выключателя снабжена ферромагнитным сердечником и имеет довольно значительную индуктивность, а выключатель снабжен блок-контактом, разрывающим ток в этой катушке при срабатывании выключателя. Как известно, энергия, выделяемая при разрыве цепи тока с индуктивностью, может быть весьма значительной. После заземления с двух сторон экрана контрольного кабеля одного из выключателей, мощность индуктированного импульса помехи на втором кабеле значительно уменьшилась, рис. 4.36, и случаи ложных срабатываний второго выключателя полностью прекратились.

Проблема с двусторонним заземлением экрана может возникнуть лишь при постоянном протекании через центральный проводник значительных по величине переменных токов, (обычно, токов промышленной частоты) вызывающих в экране значительные индуктированные токи, приводящие к его сильному нагреву. В результате приходится применять провода большего сечения (чтобы уменьшить нагрев изоляции проводов) или заземлять один из концов экрана через конденсатор. Конденсатор обладает большим сопротивлением для токов промышленной частоты и очень малым сопротивлением для высокочастотной помехи.

В некоторых случаях может возникнуть ситуация, когда через заземленный с двух сторон экран протекает значительный импульсный ток помехи, вызывающий наводку в центральной жиле. Такое может произойти, например, под действием значительного тока молнии, протекающего в близко расположенных от контрольных кабелей элементах системы заземления или под действием тока близкого короткого замыкания, рис. 4.37. Как показано в [4.18], при токе молнии в заземлителе 100 кА, даже при заземлении экрана кабеля с двух сторон, пиковое значение напряжения помехи на центральной жиле кабеля может доходить до 8.2 кВ, что значительно превосходит уровень устойчивости МУРЗ.

В этих случаях необходимо либо изменить трассу пролегания контрольных кабелей (удалить их от силовых коммутационных аппаратов, молниеотводов, разрядников), либо уменьшить разность потенциалов между заземленными концами экрана кабеля при воздействии на него мощной импульсной помехи.

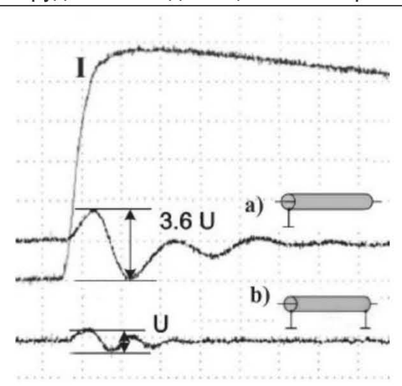


Рис. 4.37. Наводки напряжения на контрольные кабели с односторонним (a) и двусторонним (b) заземлением экрана при протекании импульса тока (I) молнии через заземлитель

Последнее решается путем прокладки вдоль кабелей медной шины, заземленной с двух сторон, которая так и называется «шиной уравнивания потенциалов». Ее действие обусловлено тем, что импеданс медной шины на высоких частотах значительно меньше импеданса земли (и даже импеданса экрана) и поэтому основная часть высокочастотного тока импульсной помехи будет протекать через эту шину, а не через экран. Разумеется, эти меры будут наиболее эффективными, если их принимать на стадии проектирования и строительства новой подстанции, а не при «латании дыр» на старой подстанции.

Контрольные кабели, естественно, должны быть экранированными и с витыми парами. Самым минимальным требованием к экрану является высокая плотность оплетки (не менее 85%). Значительно лучшим экранирующим эффектом обладают кабели с двойной оплеткой. На относительно низких частотах до нескольких десятков мегагерц оплётка обеспечивает лучшее экранирование, чем фольга, главным образом за счёт своей толщины. Однако затем экранирующие свойства оплётки резко ухудшаются и становятся почти неприемлемыми ещё до частоты 100 МГц. В то же время фольга имеет плоскую амплитудно-частотную характеристику в

области высоких частот, сохраняя удовлетворительные экранирующие способности вплоть до десятков гигагерц, рис. 4.38.

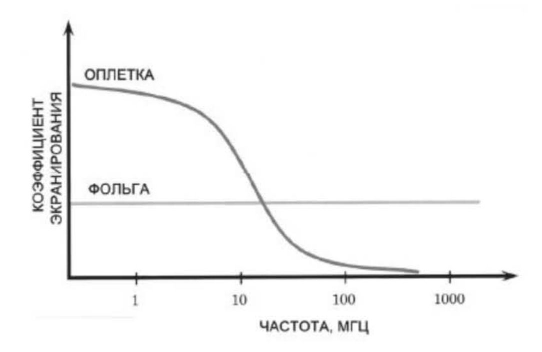


Рис. 4.38. Зависимость коэффициента экранирования от частоты для экранов в виде оплетки и фольги

Поэтому, предпочтение следует отдавать кабелям с комбинированным многослойным экраном, содержащим и оплетку, и фольгу, рис. 4.39.

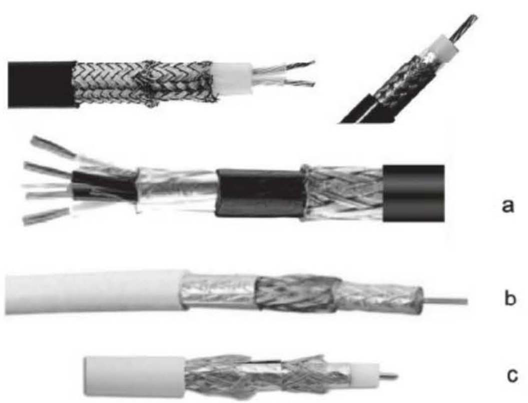


Рис. 4.39. Кабели с двойным (a), тройным (b) и четверным (c) комбинированным (оплетка-фольга) экранированием

Очевидно, что в новых проектах должны применяться специальные типы контрольных кабелей, совмещающие парную скрутку проводов и экраны из фольги для каждой такой пары с трехслойным общим комбинированным экраном (например, 48-жильный кабель типа RE-2X(ST)2Y(Z)Y PIMF), рис. 4.40.

Рис. 4.40. Кабель RE-2X(ST)2Y(Z)Y PIMF, характеризуемый как сверхустойчивый к помехам (для передачи аналоговых и цифровых сигналов до 200 Кбит/сек; парная скрутка проводов с экраном из полиэстеровой фольгой для каждой пары; трехслойный общий экран из фольги и оплетка из стальной проволоки; внешняя изоляция - сшитый полиэтилен (XLPE); до 24 пар проводов в кабеле;может применяться для прокладки на открытом воздухе и в почве; обладает высокой механической прочностью)

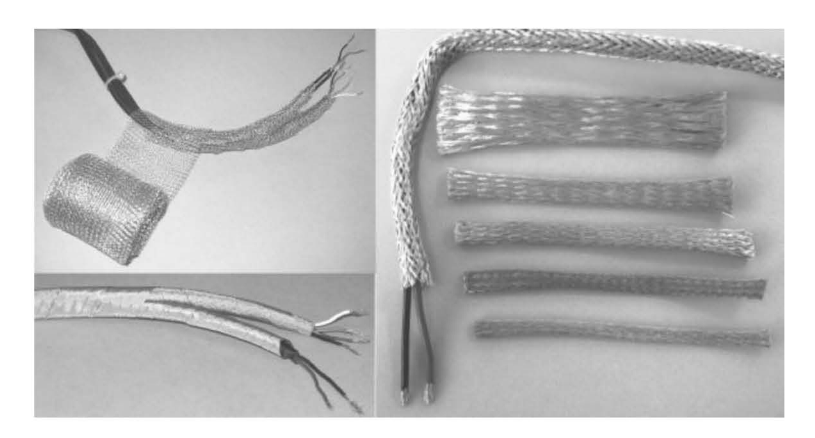


Рис. 4.41. Материалы для самостоятельного экранирования неэкранированных кабелей

Это идеальный случай, однако как быть с десятками старых контрольных кабелей, заведенных в существующие шкафы релейной защиты? Менять их на новые? Во многих случаях это бывает слишком сложно и слишком дорого. К счастью, некоторыми компаниями (например, Holland Shieldind Systems BV) выпускаются специальные сетчатые ленты, которыми могут быть просто обмотаны старые неэкранированные контрольные кабели, а также сетчатые рукава, которые могут быть натянуты на неэкранированные, а также слабо экранированные кабели, рис. 4.41.

4.6. Конструктивные изменения МУРЗ

4.6.1. Аналоговые входы

Элементами, связывающими аналоговые входы МУРЗ с внешними цепями тока и напряжения, являются входные трансформаторы тока (ТТ) и напряжения (ТН), поэтому именно эти элементы будут подвергнуты воздействию мощных перенапряжений ПДДВ в первую очередь.

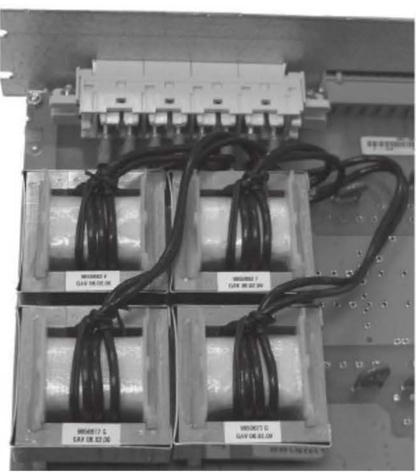


Рис. 4.42. Фрагмент модуля аналоговых входов МУРЗ с установленными ТТ. Хорошо видна первичная обмотка, состоящая из 4 витков гибкого изолированного провода черного цвета

Входные ТТ в МУРЗ имеют наиболее простую конструкцию. Как правило – это многовитковая вторичная обмотка, намотанная на ферромагнитном сердечнике и первичная обмотка, состоящая из нескольких витков толстого изолированного провода, намотанных поверх изолированной вторичной обмотки, рис. 4.42. Методы повышения устойчивости такой конструкции к воздействию мощных импульсных напряжений достаточно просты и заключаются в следующем:

- капсулирование вторичной обмотки путем заливки ее эпоксидным компаундом с отверждением под вакуумом, рис. 4.43.
- использование провода в высоковольтной изоляции для изготовления первичной обмотки;
- использование дополнительных экранов и полупроводящих покрытий, выравнивающих электрическое поле в конструкции ТТ;
- применением магнитопровода с изолированной поверхностью.

Рис. 4.43. Трансформаторы тока капсулированной конструкции с вторичной обмоткой, заложенной в пластмассовый корпус и залитой эпоксидным компаундом, отвержденным под вакуумом. Видна первичная обмотка, состоящая из одного витка гибкого изолированного провода

Десятки типов гибких проводов в высоковольтной изоляции из силикона, полиэтилена, фторопласта на напряжения 10-25 кВ выпускаются многими компаниями: Teledyne Reynolds, Multi-contact; Allied Wire & Cable; Wiremax; Dielectric Sciences Inc., Axon' Cable, Daburn Electronics & Cable, Sumitomo Electric, Belden, ОКБ Кабельной промышленности, ООО "Редкий Кабель" и многими другими.

Рекомендации по усилению устойчивости ТН аналогичны, за исключением того. что вместо гибкого провода с высоковольтной изоляцией в качестве первичной обмотки, применяется обмоточный провод с улучшенной изоляцией третьего класса в соответствии с IEC 60317-0-1 Specification for particular types of winding wires – Part 0-1: General requirements – Enamelled round copper wire из полиимида (Polyimide), а также пропитка под вакуумом обоих обмоток. Поскольку увеличение сечения обмоточного провода сопровождается автоматическим увеличением толщины изоляции и ее электрической прочности, то следует стремиться к использованию большего по сечению провода, несмотря на естественное увеличение размеров ТН. Некоторые производители выпускают обмоточные провода с изоляцией из полиимида, выдерживающие полуторное и даже двойное напряжение, по сравнению с нормируемым по стандарту IEC 60317-0-1, например, английская компания P.A.R. Insulations & Wires Ltd, турецкая Bemka A. S. и др.

4.6.2. Дискретные входы

Изоляция дискретных (логических) входов практически всех типов МУРЗ обеспечивается оптронами. Как правило, это миниатюрные оптроны в стандартных корпусах DIP-4, DIP-6, DIP-8, SOP-4. Электрическая прочность изоляции между внутренним фотоизлучающим и фотопремным элементами у таких оптронов может доходить до 5 - 7 кВ действующего значения переменного тока. Однако реально оптроны, установленные на печатной плате, такие напряжения не выдержат из-за пробоя между ножками по поверхности платы. В то же время, на рынке широко представлены оптроны в специальных корпусах с разнесенными в пространстве выводами входа и выхода, рис. 4.44, выдерживающие напряжения между входом и выходом, доходящее до 12 – 25 кВ. Это оптроны типа OC100 (Voltage Multipliers, Inc.); HV801 (Amptec, Inc.); OPI1268S

(TT Electronics); 5253003120 (Standex Meder Electronics) и др. Именно такие оптроны следует применять в дискретных входах МУРЗ для повышения их устойчивости к ЭМИ ЯВ.

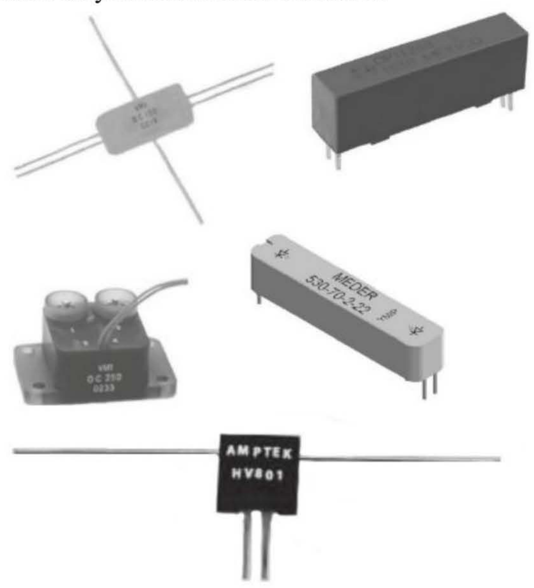


Рис. 4.44. Внешний вид оптронов некоторых типов с напряжением изоляции входа от выхода 12 – 25 кВ

Схемы МУРЗ обычно построены таким образом, что первыми элементами, к которым прикладывается поступающий на дискретные входы сигнал, являются варисторы, защищающих входы оптронов от перенапряжений. Далее следуют гасящие высокоомные резисторы, снижающих уровень входного напряжения (обычно, это 230 В постоянного тока) до рабочего напряжения входной цепи оптрона, при котором ток в этой цепи не превышает нескольких миллиампер. При использовании TVS-диодов (см. выше) вместо варисторов, дискретные входы оказываются хорошо защищенными не только от коммутационных перенапряжений, как при использовании варисторов, но и от короткого высоковольтного импульса компонента E1 ЭМИ ЯВ, если ему удастся проникнуть на эти входы. Слишком высокое быстродействие современных оптронов, особен-

но на основе фотодиодов, которое может достигать 10^{-9} секунды, является еще одной проблемой. Поэтому с целью повышения помехоустойчивости оптрона требуется дополнительная защита от его ложного срабатывания при воздействии короткого импульса E1, которая может быть осуществлена путем шунтирования входа оптрона высокочастотным керамическим конденсатором, снижающим быстродействие оптрона и таким образом повышающим его помехоустойчивость.

4.6.3. Выходные реле

Использование в МУРЗ выходных реле с повышенной прочностью электрической изоляции является одной из мер повышении устойчивости МУРЗ к воздействию ЭМИ ЯВ.

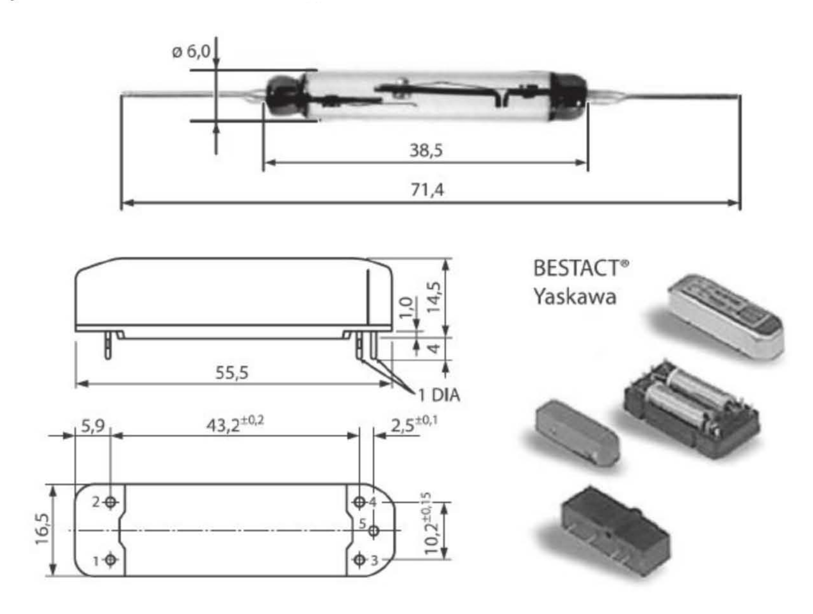


Рис. 4.45. Мощный геркон типа R14U (R15U) с двойным контактом и реле на его основе, производимые компанией Yaskawa

Хорошие перспективы имеет использование герконовых реле, выполненных на основе новых малогабаритных герконов большой мощности типа R14U и R15U, с двойной коммутацией, производимого компанией Yaskawa, под торговой маркой BESTACT®, рис. 4.45. Герконы этого типа имеют двойной контакт (основной и дугогасительный), с последовательной коммутацией, позволяющий включать активно-индуктивную нагрузку с током 15А при напряжении 220В постоянного тока и 30А при напряжении 220В переменного тока. На основе этих герконов компания выпускает реле различных типов, например, типа R1-B14T2U. Одним из отличий герконового реле от других типов электромагнитных реле является простота конструкции (геркон и катушка) и возможность простыми техническими средствами обеспечить очень высокий уровень изоляции (десятки киловольт) между катушкой и герконом. Такая возможность герконового реле очень важна при использовании его в качестве выходного реле МУРЗ, защищенного от ЭМИ ЯВ, и она может быть реализована на основе готовых разработок автора, описанных в [4.19].

4.6.4. Печатные платы

Устойчивость к импульсным напряжениям современных печатных плат с элементами поверхностного монтажа зависит не только от правильного выбора электронных компонентов, но и от пробивного напряжения между ножками элементов и расстояния между печатными проводниками (которые из-за высокой плотности монтажа бывают очень маленькими). Поэтому, одним из дополнительных путей повышения надежности МУРЗ в условиях воздействия ЭМИ ЯВ может быть сплошное двустороннее покрытие плат специальным высоковольтным лаком. Примером такого лака могут быть продукты, выпускаемые компанией Vol Roll под торговой маркой Damicoat® , типов 2405-01, 2407-01 и др. Эти лаки имеют электрическую прочность изоляции 70 – 100 кВ/мм. Поскольку печатные платы с таким покрытием становятся полностью неремонтопригодными, то отсюда вытекает дополнительное требование к конструкции МУРЗ: количество печатных плат, из которых состоит МУРЗ, должно быть увеличено с тем, чтобы при выходе из строя какого-то одного функционального модуля заменять только этот

один модуль, а не большую группу функциональных модулей, расположенных на общей печатной плате. Для этого количество печатных плат, из которых состоит МУРЗ, должно быть увеличено до количества функциональных модулей. То есть, каждый функциональный модуль (источник питания, модули дискретных входов, модули аналоговых входов, модуль центрального процессора, модуль выходных реле) должен быть выполнен на отдельной выдвижной печатной плате, соединяемой с другими платами посредством соединителя через кросс плату.

Такой подход является не только необходимым в связи с неремонтопригодностью отдельных модулей МУРЗ с изоляционным покрытием, но и весьма желательным, поскольку помогает решению проблемы стандартизации конструкции МУРЗ и универсализации его модулей [4.20].

Еще одним преимуществом такой конструкции МУРЗ, состоящей из отдельных неремонтопригодных функциональных модулей, является возможность использования нового (для релейной защиты) критерия оценки надежности, вместо такого, мягко выражаясь, странного критерия, как «наработка на отказ» с его фантастическими цифрами в 50 – 90 лет, которые не имеют никакого отношения к реальной (а не фиктивной) надежности. Этот критерий называется ***«гамма-процентной наработки до отказа»*** и характеризует собой наработку, в течение которой отказ объекта не возникает с определенной вероятностью, выраженной в процентах. Например, 95%-ная наработка до отказа в течение не менее 5 лет означает, что за 5 лет работы должно отказывать не более 5% устройств находящихся в эксплуатации. Имея такой удобный и понятный показатель, потребитель мог бы отследить количество вышедших из строя модулей за определенный промежуток времени и предъявить производителю претензии, если в течение этого промежутка отказало значительно большее количество модулей, чем это было гарантировано производителем. Имея такой показатель, потребителю будет значительно легче ориентироваться и на будущем рыке универсальных модулей [4.20], выбирая для себя наиболее приемлемый вариант, по соотношению цена/качество. В дополнение к этому, от производителей необходимо потребовать указания в технической и тендерной документации среднего срока службы отдельных модулей и рекомендации относительно периодичности превентивной замены этих

модулей с целью поддержания высокого уровня надежности релейной защиты. Например, для модуля источника питания это может быть 8-10 лет; для модуля логических входов – 12 лет; для модуля центрального процессора – 15 лет; для модуля аналоговых входов – 17 лет, и т.д. Эти данные должны быть известны добросовестному производителю, отслеживающему статистику отказов и повреждений своих изделий.

4.7. Строительные материалы

Одним из таких видов защит является защита зданий и отдельных помещений от проникновения ЭМИ. Наиболее мощной является защита с использованием специальных панелей, содержащих и отражающие и поглощающие ЭМИ слои, рис. 4.46.

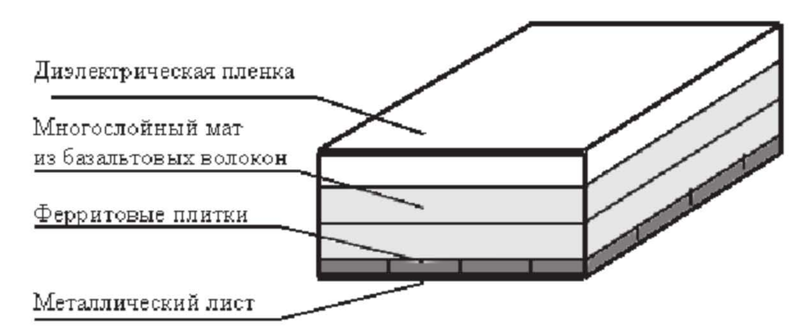


Рис. 4.46. Структура интегрированной панели “Феррилар-5”для защищенного помещения

Однако, создание полностью экранированного помещения является достаточно дорогим мероприятием. Поэтому, на практике представляют определенный интерес более дешевые промежуточные варианты с использованием, например, защитной краски, пленки, штор, драпировок и т.п. За последние годы существенные результаты достигнуты в области создания электропроводных лакокрасочных и строительных материалов с уникальными свойствами и широкими возможностями применения, а также прозрачных токопроводящих покрытий, которые могут быть нанесены на стекло.

Электропроводные краски, лаки и спреи на основе меди, алюминия, бронзы, никеля и графита выпускаются многими фирмами, например, Caswell, YSHIELD EMR-protection Company, Less EMF Inc, Gold Touch, Inc., Spraylat Corp., Cybershield, Applied Coating Technologies Ltd, BM Industria Bergamasca Mobili S.p.A. Хорошими показателями обладает защитная краска “Тиколак” московской фирмы «Тико». «Тиколак» - новый универсальный неметаллический электропроводный лакокрасочный материал, защищенный патентом Российской Федерации, представляющий собой смесь углеродосодержащего наполнителя и полимерного связующего в соотношении: эпоксидное связующее 8-20% наполнитель смесь графита с сажей при массовом соотношении 0,1:1,0:11-39% отвердитель 0,5-1,5% органический растворитель остальное. По данным фирмы Тико «Тиколак» способен экранировать электромагнитые излучения в широком диапазоне частот вплоть до 300 ГГц. «Тиколак», нанесенный на внутренние или внешние поверхности зданий, во много раз снижает проникающую способность электромагнитного излучения (по данным разработчика один слой “Тиколака” толщиной всего в 70 мкм снижает интенсивность ЭМИ в 3 – 3,5 раза). «Тиколак» можно наносить на различные строительные материалы - ДСП, дерево, фанеру, гипсовые плиты, а также на любой гибкий материал - ткань, кожу, пленки, бумагу и др. На покрытие из «Тиколак» можно наносить любой отделочный материал - обои, краску, керамическую плитку и т.д., при этом «Тиколак» стоит намного меньше зарубежных аналогов (около 70 долларов США за 1 кг).

Для получения прозрачного электропроводного стекла, отражающего ЭМИ, используют полупроводниковые пленки оксидов различных металлов: олова, индия, цинка и др. Технология изготовления таких стекол очень сложная, трудоемкая и требует дорогостоящего оборудования и квалифицированного персонала. Уже упомянутой фирмой Тико разработан и запатентован (патент РФ № 2112076) высокотехнологичный и экономичный способ нанесения на стекло электропроводящих покрытий на основе оксидов индия и олова. Прозрачное электропроводящее стекло производится многими компаниями, например, Tycon Technoglass, Pilkington, Shenzhen Wanyelong Industry Co., Ltd, InkTec и др.

Компанией Альфапол из Санкт-Петербурга на основе шунгитовых пород созданы стройматериалы, совмещающие в себе свойства

обычных стройматериалов и достаточно высокую электропроводность. Это определяет способность материала экранировать электромагнитные излучения. По данным компании Альфапол, шунгитовые композиционные радиоэкранирующие материалы по способам реализации из них экранов могут быть разделены на два класса:

- конструкционные материалы, к числу которых относится бетон, кирпич, кладочный раствор. Материалы способны обеспечить ослабление электромагнитной энергии в диапазоне частот более 100 МГц на уровне не менее 100 дБ. По физико-механическим характеристикам шунгитовые конструкционные материалы не уступают традиционным строительным аналогам.

Рис. 4.47. Электропроводные пленки, нити и ткани, ослабляющие ЭМИ (до 80 дБ), производимые компанией Koolon Fiber Tech. Corp.

Шунгитовые материалы прошли испытания в конструкциях (бетон в панелях перекрытий, кирпич в кладках) и признаны соответствующими существующим требованиям.

- материалы для реконструкции, такие как штукатурные растворы и мастики, позволяющие переоборудовать обычные сооружения в экранированные. Мастики способны обеспечить экранирующий эффект на уровне не менее 30 дБ в диапазоне свыше 30 МГц при

толщине слоя в 2-3 см. А штукатурный состав «Альфапол ШТ-1» при толщине слоя штукатурки 15 мм в диапазоне частот от 10 кГц до 35 ГГц обеспечивает ослабление ЭМИ на 10 – 15 дБ.

Шунгит - группа твердых углеродистых минеральных веществ, представляющих в главной массе аморфные разновидности углерода, близкие по составу к графиту. Химический состав шунгита непостоянен: в среднем содержит 60 - 70 % углерода и 30-40% золы. В золе содержится: 35-50% окиси кремния, 10-25 % окиси алюминия, 4-6% окиси калия, 1-5 % окиси натрия, 1-4% окиси титана, а также примеси других элементов.

В качестве дополнения к стенам помещений, содержащих шунгит, можно использовать электропроводные шторы и ткани, напольные покрытия, производимые некоторыми фирмами, рис. 4.47.

Литература к Гл. 4

4.1 Whitaker J. C. Electronic Systems Maintenance Handbook, Second Edition - CRC Press (Taylor & Francis Group), Boca Raton – New York – London, 2001, 624 p.

4.2 Ильин В. Ф., Ильин Н. В. Заземление в шкафах микропроцессорных защит. – Релейная защита и автоматизация, 2015, № 1, с. 26-30.

4.3 Гуревич В. И. Уязвимости микропроцессорных реле защиты. Проблемы и решения. – М.: Инфра-Инженерия, 2014.- 256 с.

4.4 Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C41SR) Facilities. Technical Manual TM 5-690. Headquarters Department of the Army, 17 February 2002.

4.5 IEC 60364-5-548: 1999. Electrical installations of buildings - Part 5: Selections and erection of electrical equipment - Section 548: Farthing arrangements and equiponential bounding for information technology installations.

4.6 MIL-STD-188-125-1 High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Per-

forming Critical, Time-Urgent Missions; Part 1: Fixed Facilities.

4.7 A. J. Nalhorczyk, HEMP Filter Design to Meet MIL-STD-188-125 PCI Test Requirements. – IEEE. 10-th International Conference “Electromagnetic Interference & Compatibility”, 26-27 Nov., 2008, pp. 205 – 209.

4.8 MIL-STD-461F Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 2007.

4.9 IEC 61000-4-4 Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test, 2012.

4.10 Application Notes Cat. 1: HEMP Filter Maintenance and Monitoring. Rev.1. MPE Ltd., December, 2012.

4.11 Surge Protective Device Response Time, Application Note 9910-0003A, Schneider Electric, August 2011.

4.12 Power Quality Surge Protective Devices (SPD), Application Notes: Response Time ratings, DET-733 (8/10), General Electric.

4.13 Surface Mount Power TVS Diodes Deliver Optimal Protection for Power Supply. Application Note, Bourns, Inc, 7/14.e/ESD1435.

4.14 S. J. Goldman, Selecting Protection Devices: TVS Diodes vs. Metal-Oxide Varistors, Power Electronics, June 1, 2010.

4.15 IEC 61000-4-25:2001 Electromagnetic compatibility (EMC) - Part 4-25: Testing and measurement techniques - HEMP immunity test methods for equipment and systems

4.16 Гуревич В. И. Проблемы тестирования микропроцесссорных реле защиты на устойчивость к преднамеренным электромагнитным деструктивным воздействиям. - "Компоненты и технологии", 2014, № 12, с. 161 - 168.

4.17 MIL-STD-220B Method of Insertion Loss Measurement, Department of Defense, 1959.

4.18 Кузнецов М. Б., Кунгуров Д. А., Матвеев М. В., Тарасов В. Н. Проблемы защиты входных цепей аппаратуры РЗА от мощ-

ных импульсных перенапряжений. - Relay Protection and Substation Automation of Modern EHV Power Systems (Moscow – Cheboksary, September 10–12, 2007).

4.19 Gurevich V. Protection Devices and Systems for High-Voltage Applications. Marcel Dekker, New York, 2003, 292 p.

4.20 Гуревич В. И. Проблемы стандартизации в релейной защите. – СПб: Издательство ДЕАН, 2015. – 168 с.

5. АКТИВНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ МУРЗ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

5.1. Новый принцип активной защиты МУРЗ

В структуре современной энергосистемы МУРЗ являются самым критичным звеном [5.1], поскольку с одной стороны наиболее уязвимы к преднамеренным дистанционным деструктивным воздействиям (ПДДВ), а с другой – непосредственно связаны с силовыми коммутационными аппаратами, влияющими на состояние энергосистемы. Поэтому именно на МУРЗ и направлены в первую очередь ПДДВ в виде кибератак [5.2] и преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) [5.3].

Осознание проблемы кибербезопасности МУРЗ в последние годы привело к интенсификации многочисленных исследовательских работ, связанных, в основном, с совершенствованием компьютерных протоколов связи, предназначенных для релейной защиты и повышением их криптостойкости. До недавнего времени именно в этом направлении и были сосредоточены все усилия специалистов. Что касается ПЭДВ, то как показано в Гл. 1 этой проблемой, похоже, пока вообще никто **серьезно** не занимается. Между тем, еще 17 лет тому назад, когда проблемы МУРЗ лишь начали вырисовываться, автором была предложена в общем виде идея высокоэффективной комбинированной защиты МУРЗ и от кибератак и от ПЭДВ с помощью аппаратных, а не программных средств. Это устройство защиты, работающее на принципе шунтирования чувствительных входов МУРЗ с посредством быстродействующих электромеханических реле на герконах [5.6]. В последующем, идея применения быстродействующих электромеханических реле на герконах совместно с МУРЗ для снижения их уязвимости к ПДДВ была проработана автором более тщательно [5.7, 5.8].

Как нами уже было неоднократно показано ранее, ***задачу повышения надежности релейной защиты невозможно решить при совмещении функций МУРЗ с функциями, не имеющими отношения к РЗ,*** например таких популярных, как мониторинг исправности электрооборудования, дистанционное управление выключателями и т.п. МУРЗ должны использоваться исключительно

для решения задач релейной защиты. Тем более, что для решения других задач, например, для мониторинга электрооборудования, сегодня на рынке имеется огромное количество специализированных устройств, от простейших реле, контролирующих целостность цепи отключающей катушки выключателя, до сложнейших комплексов, контролирующих в режиме реального времени состав газов, растворенных в масле трансформаторов или уровень частичных разрядов в изоляции. Что касается дистанционного управления выключателями посредством МУРЗ, то при таком его использовании очень трудно отличить санкционированный дистанционный доступ от несанкционированного, поэтому такое использование МУРЗ должно быть исключено. Тем более, что при разделении функций удается достаточно простыми аппаратными средствами обеспечить защиту от ПДДВ и системы дистанционного управления выключателями (см. ниже).

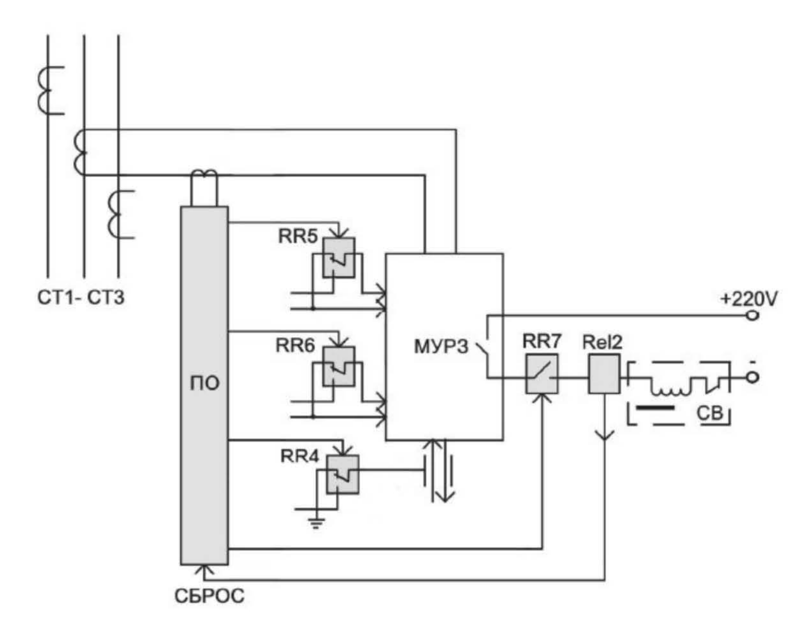


Рис. 5.1. Структурная схема устройства защиты МУРЗ от ПДДВ

Общая идея, лежащая в основе предлагаемого аппаратного метода защиты МУРЗ от ПДДВ, заключается в использовании совместно с МУРЗ электромеханического пускового органа на герконах (ПО), функционально включенного последовательно с МУРЗ, и быстродействующих электромеханических исполнительных элементов (RR1 – RR7), обеспечивающих блокировку чувствительных входов МУРЗ и отключение его выходной цепи, рис. 5.1. Возврат сработавшего ПО в исходное состояние осуществляется по факту срабатывания выключателя и дублируется командой СБРОС по истечении заранее заданного небольшого промежутка времени. Без активации током и/или напряжением такого пускового органа, МУРЗ не сможет воздействовать на режим работы энергосистемы, даже будучи подвергнутым воздействию ПДДВ или просто мощной электромагнитной помехи. Если же пусковой орган был активирован и МУРЗ деблокирован, то ничего не мешает использованию особых характеристик и широких функциональных возможностей МУРЗ. При этом излишние срабатывания самого пускового органа никак не влияют на работу релейной защиты и поэтому никаких особых требований к точности срабатывания пускового органа не предъявляется. Важно лишь, чтобы он срабатывал всегда до МУРЗ, то есть имел несколько меньшие уставки срабатывания по контролируемому параметру. Если срабатывание пускового органа оказалось излишним и срабатывания МУРЗ не произошло, то устройство автоматически возвращается в исходное состояние. Основными техническими требованиями к такому устройству являются его высокая надежность, нечувствительность к коротким импульсным (микро- и наносекундного диапазона) и высокочастотным помехам, стойкость к значительным перенапряжениям, высокий уровень гальванической развязки от внешних цепей, высокое быстродействие на срабатывание (несколько миллисекунд). Герконы – это именно те элементы, которые позволяют простыми техническими средствами решить эти задачи.

В данной главе приведено описание усовершенствованного устройства, предназначенного для защиты МУРЗ от ПДДВ, удовлетворяющего сформулированным выше требованиям, рис. 5.2.

Работает устройство следующим образом. В исходном состоянии, при нормальном режиме работы защищаемого объекта, все

входные герконовые реле (датчики тока, напряжения и т.д.) RR1-RR3 находятся в отпущенном состоянии.

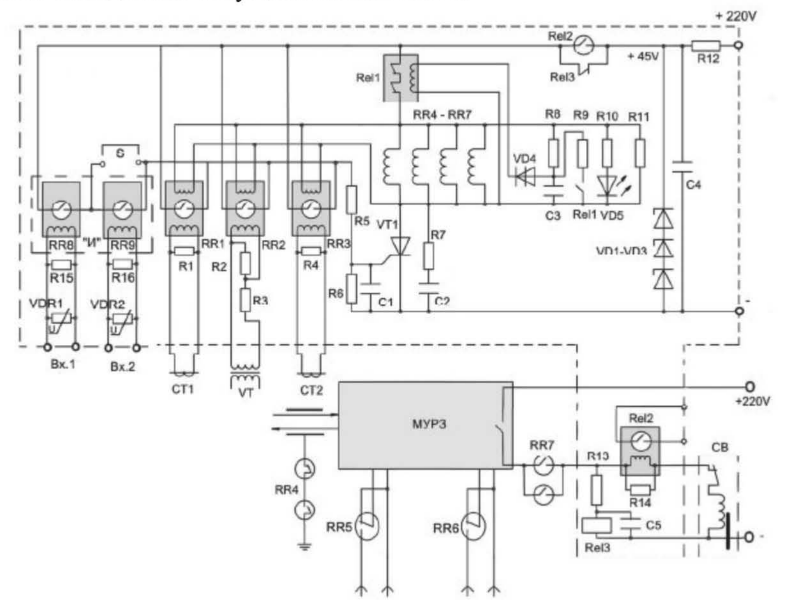


Рис. 5.2. Усовершенствованная схема устройства защиты МУРЗ от ПДДВ

Тиристор VT1 заперт, катушки исполнительных герконовых реле RR4-RR7 обесточены. Нормально замкнутые контакты RR5 и RR6 отключают и закорачивают логические входы МУРЗ, контакты RR4 - канал связи, а контакты RR7 разрывают выходную цепь МУРЗ. Таким образом, в этом состоянии МУРЗ оказывается полностью заблокирован и по входу и по выходу и никакие ПДДВ или кибератаки не могут привести к ложному его срабатыванию и несанкционированному замыканию цепи отключающей катушки выключателя CB. Шунтирование логических входов МУРЗ и канала связи повышает также его живучесть при воздействии мощного электромагнитного импульса.

При возникновении аварийного режима защищаемого объекта, хотя бы один из контролируемых параметров (ток, напряжение, мощность) резко изменяется. Это изменение приводит к срабатыванию хотя бы одного из герконовых реле RR1- RR3 за время не более 1 мс. При срабатывании начинает вибрировать с удвоенной частотой сети геркон соответствующего реле. При первом же замыкании контактов этого геркона мгновенно отпирается тиристор VT1 и катушки исполнительных герконовых реле RR4-RR7 получают питание. Срабатывание реле RR4-RR6 происходит за время не более 4 мс, а замыкание мощных контактов герконового реле RR7 на герконе типа Bestact R15U – за время не более 5 мс. Таким образом, суммарное время реакции всего устройства на аварийный режим не превышает 6 мс, что при собственном минимальном времени срабатывания МУРЗ порядка 30-40 мс вполне приемлемо. В таком режиме работы МУРЗ будет полностью разблокировано и возвращено в нормальный режим функционирования с сохранением всех его уставок и характеристик.

Как видно на схеме рис. 5.2, каждое из входных реле (датчиков) снабжено второй обмоткой на герконе, которая получает питание от источника постоянного напряжения при отпирании тиристора VT1. Благодаря дополнительному магнитному полю, создаваемому этой обмоткой, геркон сработавшего реле перестает вибрировать и переходит в стабильное замкнутое состояние.

После того, как МУРЗ отработает заданную его характеристикой выдержку времени, его внутренний выходной контакт замкнется и подаст напряжение на отключающую катушку выключателя CB. Ток, протекающий в цепи отключающей катушки выключателя, приводит к срабатыванию герконового реле Rel2 с мощным герконом типа Bestact R15U и замыканию его контактов, включенных параллельно нормально замкнутым контактам Rel3. С некоторой очень небольшой задержкой по времени (порядка 20-50 мс), срабатывает реле Rel3. Эта выдержка времени необходима для того, чтобы контакт реле Rel2 всегда замыкался до размыкания контакта Rel3.

В конце цикла срабатывания выключателя CB размыкается его блок-контакт и разрывается цепь питания отключающей катушки. При этом отпускает реле Rel2 и его контакт разрывает анодную цепь тиристора VT1, который при этом мгновенно запирается, обес-

точивая обмотки реле RR4-RR7 и обмотки постоянного тока реле RR1- RR3. Все устройство быстро возвращается в исходное состояние и готово к новому циклу работы.

Если срабатывание устройства оказалось излишним и МУРЗ не выдало команду на отключение выключателя, цепь питания тиристора VT1 будет кратковременно разорвана нормально замкнутым контактом реле Rel1, после заряда конденсатора C3 через резистор R8 и отпирания динистора VD4. Емкость этого конденсатора и сопротивление резистора обеспечивают выдержку времени в несколько секунд, превышающую максимально возможное время, необходимое для завершения полного цикла работы МУРЗ, чтобы не мешать его работе, если она необходима. Срабатывание реле Rel1 кратковременное, поскольку сразу после его срабатывания и размыкания нормально замкнутого контакта в цепи тиристора, замыкается его нормально разомкнутый контакт и разряжает конденсатор C3 через низкоомный резистор R9, обеспечивая его полный разряд и возврат в исходное состояние. При этом динистор VD4 запирается и катушка реле Rel1 обесточивается. Таким образом осуществляется принудительный возврат устройства в исходное состояние, если его срабатывание оказалось излишним.

Резистор R11 необходим для увеличения тока, протекающего через мощный тиристор VT1 и его надежного удержания в проводящем состоянии. Светодиод VD5 является индикатором состояния устройства.

Контакты внешних реле, предназначенные для активации/дезактивации внутренних функций МУРЗ, определяющих состояние релейной защиты, должны включаться помимо защищенных (зашунтированных в нормально режиме) логических входов МУРЗ, показанных на рис. 5.2, еще и на логические входы (Вх.1, Вх.2) описанного устройства защиты. При этом, с целью повышения защищенности системы, необходимо наличие не менее двух входных сигналов об одном событии, поступающих от двух источников. Внутри устройства защиты эти сигналы гальванически изолируются от внешних цепей дополнительными герконовыми реле RR7, RR8, посредством которых реализуется также логическая функция «И», результатом действия которой является активация устройства защиты и деблокирование всех логических входов для выполнения необходимых операций. Причем не обязательно оба

эти источника должны быть в виде дискретных сигналов (контактов реле). Один из них может быть дискретным сигналом, а другой – аналоговым, в виде тока или напряжения, поступающего на соответствующее входное герконовое реле, выходные контакты которых включены по логической схеме «И». При этом выход реле второго (неиспользуемого) логического входа может быть зашунтирован перемычкой S.

Устойчивость этих дополнительных логических входов к коротким импульсным помехам даже очень большой амплитуды обеспечивается соответствующим уровнем изоляции между обмоткой и герконом и наличием собственного времени срабатывания геркона. Последний не может сработать за время меньшее нескольких миллисекунд и таким образом является естественным и очень эффективным фильтром высокочастотных и импульсных помех.

С целью обеспечения необходимой помехоустойчивости ко всякого рода переходным процессам в цепях питания постоянного оперативного тока эти дополнительные входы должны иметь входное сопротивление значительно более низкое, чем обычные логические входы МУРЗ, что достигается шунтированием их внутренними резисторами R15 и R16.

Хотя обмотки входных герконовых реле значительно более устойчивы к перенапряжениям, чем полупроводниковые приборы, в устройстве приняты меры для дополнительно защиты их от перенапряжений, возникающих при ПЭДВ, с помощью варисторов VDR1, VDR2.

Конструктивно устройство защиты выполнено в экранированном корпусе, аналогичном корпусам МУРЗ с той лишь разницей, что в нем нет экрана, но имеется доступ к узлам регулирования порога срабатывания герконовых реле пускового органа.

С целью повышения надежности устройства и его стойкости к ПЭДВ в нем применено всего лишь несколько полупроводниковых приборов и они выбраны с очень большими запасами по напряжению и току, которые в обычной аппаратуре промышленного назначения не применяются. Так, например, при рабочем напряжении 45 В, тиристор VT1 выбран на максимальное напряжение 1200 В, при рабочем токе в доли ампера он способен работать при токах в десятки ампер и пропускать кратковременные импульсы тока в сотни ампер. С многократными запасами по мощности выбраны также

стабилироны VD1-VD3 и динистор VD4. Промежуточные реле Rel1 и Rel3 выбраны герметичными с контактами повышенной мощности.

Ниже приведены общие рекомендации по выбору элементной базы для предлагаемого устройства активной защиты.

В качестве чувствительного порогового элемента в пусковом органе могут быть использованы миниатюрные вакуумные герконы, выдерживающие испытательное напряжение не менее 1 кВ и имеющие собственное время срабатывания около 1 мс, табл. 5.1.

Табл. 5.1. Основные параметры быстродействующих вакуумных высоковольтных герконов некоторых типов

Параметр/Тип геркона	**MRA 5650G**	**KSK-1A75**	**HYR 2016**	**HYR 1559**	**MARR-5**	**KSK-1A85**
Тип контакта	NO	NO	NO	NO	NO	NO
Коммутируемое напряжение, В	1000	1000	1000	1500	1000	1000
Коммутируемый ток, А	1	0.5	1	0.5	0.5	1
Коммутируемая мощность, Вт	100	10	25	10	10	100
Пробивное напряжение, В	1500	1500	2500	1500	2000	4000
Время замыкания, мс	0.6	0.5	0.8	0.4	0.75	1.0
Время размыкания, мс	0.05	0.1	0.3	0.2	0.3	0.1
Размеры, мм	D =2.75 L=21	D=2.3 L=14.2	D=2.6 L=21	D=2.3 L=14.2	D=2.66 L=19.7	D=2.75 L=21
Чувствительность, ампер-витков	20 – 60	15 - 40	15 -70	15 - 50	17 - 38	20 – 60

Поскольку для работы МУРЗ в аварийном режиме защищаемого объекта необходимо время, не превышающее обычно нескольких секунд, то время возврата около 5-10 сек схемы в ждущий режим

вполне достаточно для полного завершения цикла нормальной работы МУРЗ.

Табл. 5.2. Важнейшие параметры некоторых типов высоковольтных тиристоров, предназначенных для распайки на печатную плату

Параметр / Тип	CLA50E-1200HB	25TTS12	30TPS12 30TPS16	BTW68-1200
V_{RRM}/V_{DRM}, V	1200	1200	1200 1600	1200
$I_{T\,(RMS)}$, A	79	25	30	30
$I_{T\,(AV)}$, A	50	16	20	19
I_{TSM}, A	650	300	250	400
I_{GT}, mA	50	60	45	50
I_L, max., mA	125	200	200	40
I_H, max., mA	100	100	100	75
dv/dt, V/µs	1000	500	500	250
T_{GT}, µs	2	0.9	0.9	100
T_J, °C	-40 +150	-40 +125	-40 +125	-40 +125
Корпус	TO-247	TO-220AC	TO-247AC	TOP3 ins.

Продолжение **Табл. 5.2.**

Параметр / Тип	CS 20-12io1 CS 20-14io1 CS 20-16io1	CS 30-12io1 CS 30-14io1 CS 30-16io1	CS 45-12io1 CS 45-16io1
V_{RRM}/V_{DRM}, V	1200 1400 1600	1200 1400 1600	1200 1600
$I_{T\,(RMS)}$, A	30	49	75
$I_{T\,(AV)}$, A	19	31	48
I_{TSM}, A	200	300	520
I_{GT}, mA	65	65	100
I_L, max., mA	150	150	150
I_H, max., mA	100	100	100
dv/dt, V/µs	1000	1000	1000
T_{GT}, µs	2	2	2
T_J, °C	-40 +125	-40 +125	-40+140
Корпус	TO-247AD	TO-247AD	TO-247AD

Поскольку суммарный ток, потребляемый обмотками исполнительных реле RR4 – RR7, может оказаться меньше тока защелкивания (I_L) и тока удержания (I_H) тиристора VT1, схема рис. 5.2 дополнена мощным резистором R11, увеличивающим суммарный ток,

протекающий через тиристор до 250-300 мА. Хотя на рынке имеются специальные тиристоры с повышенной чувствительностью и с токами защелкивания и удержания не превышающими 10 мА (TS820-600, TIC106, BT258-600R, X0402MF, MCR708A1 и др.), их применение в данной устройстве не рекомендуется, так как это может снизить его помехоустойчивость.

В табл. 5.2 приведены параметры некоторых типов наиболее подходящих для использования в пусковом органе тиристоров. Для повышения помехоустойчивости пускового органа в нем применены дополнительные RC-элементы.

В качестве контактов исполнительных реле, блокирующих выходной контакт МУРЗ, могут быть с успехом использованы газонаполненные герконы Bestact R15U фирмы Yaskawa, рис. 7.3, предназначенные для включения токов до 30А при напряжении 240 В за время, не превышающее 5 мс.

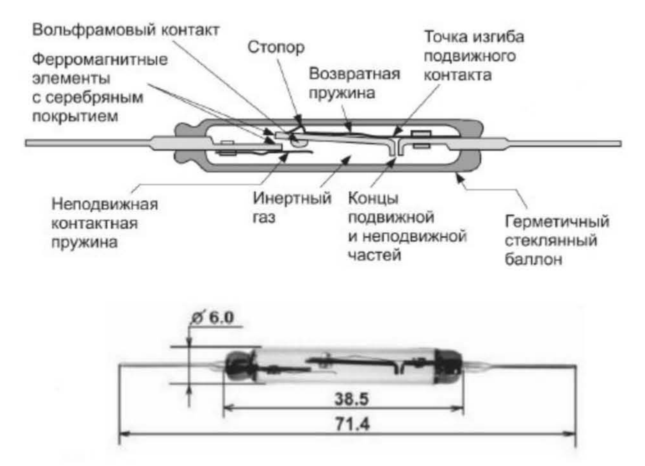


Рис. 5.3. Мощный газонаполненный геркон типа Bestact R15U фирмы Yaskawa с двустадийной коммутацией

Высоковольтные миниатюрные вакуумные переключающие герконы различных типов, содержащие нормально замкнутый контакт, табл. 5.3, могут быть использованы для шунтирования чувствительных (не токовых) входов МУРЗ.

У электромеханических реле вероятность отказов типа «излишние срабатывания» несравненно меньше вероятности «несрабатывания», поэтому их параллельное соединение (в отличие от простого параллельного соединения МУРЗ) однозначно увеличит надежность релейной защиты.

Для нормально замкнутых дополнительных контактов шунтирующих входы МУРЗ, повышение надежности может быть достигнуто последовательным соединением этих контактов между собой.

Табл. 5.3. Основные параметры некоторых типов герконов с переключающим контактом

Параметр / Тип и производитель	GC 1917 Comus	HSR-830R Hermetic Switch	HSR-834 Hermetic Switch,	HSR-V933W Hermetic Switch	DRR-DTH Hamlin
Max. коммутируемая мощность, Вт	60	25	100	100	50
Max. коммутируемое напряжение, В	400	250	500	500	500
Max. коммутируемый ток, А	1	1	3	3	0.5
Пробивное напряжение, В	1000	1000	1000	1500	1200
Время замыкания, мс	4.0	3.6	2.0	4.2	4.5
Время размыкания, мс	0.15	4.2	1.0	3.7	7.0
Размеры баллона, мм	D=5.6, L=36	D=5.3, L=32	D=5.3, L=34	D=5.3, L=33	D=5.5 L=39.7

Конденсатор времязадающей цепочки, как и все остальные элементы устройства, выбран улучшенного качества и с большим запасом (пятикратным) по рабочему напряжению, табл. 5.4.

В качестве делителя напряжения выбраны три последовательно включенных стабилитрона VD1 – VD3 с напряжением стабилизации 15 В, мощностью 10 Ватт каждый.

Табл. 5.4. Основные параметры некоторых типов высококачественных конденсаторов для времязадающей цепочки

Тип конденсатора	Производитель	Емкость и напряжение	Габаритные размеры, мм	Рабочая температура, °C
B43504B2477M	EPCOS	470 µF, 250V	Dia.30 x 30	-40 +105
B43505A2477M	EPCOS	470 µF, 250V	Dia.30 x 35	-40 +105
EETHC2E471CA	Panasonic	470 µF, 250V	Dia.25 x 30	-40 +105
MAL215933471E3	Vishay	470 µF, 250V	Dia.25 x 40	-25 +105
MCHPR250V477M25X41	Multicomp	470 µF, 250V	Dia.25 x 41	-25 +105
381LQ471M250J022	Cornell Dublier	470 µF, 250V	Dia.25 x 30	-40 +105

Табл. 5.5. Основные параметры некоторых типов стабилитронов мощностью 10-20 Ватт с напряжением стабилизации 15 В

ПАРАМЕТР / ТИП	NTE5191A	1N2979	BZY93-C15
P_D, W	10	10	20
V_Z, V	15	15	15
I_{ZM}, mA	560	560	1000
I_{ZT}	170	170	170
Z_{ZT}, Ω	3	3	1.2
I_R, µA	10	5	50
T_{OPR}, °C	-65+175	-65+175	-55+175
Тип корпуса	DO-4	DO-4	DO-4

При очень небольшом собственном потреблении схемы, большой запас по мощности обеспечивает отсутствие нагрева стабилитронов и повышение надежности их работы, а также способности поглощать импульсы перенапряжения большой энергии. Параметры наиболее подходящих для этой цели стабилитронов приведены в табл. 5.5.

В качестве динистора VD4 (рис. 5.2) с напряжением отпирания 24 – 36 В и пропускаемым током 1 – 2 А могут быть рекомендованы приборы следующих типов: NTE6407, DB3, BR100/03, CT-32, HT-32 и др. А в качестве электромагнитного реле Rel (рис. 7.2) - герме-

тичные нейтральные электромагнитные реле (в англоязычной технической литературе они называются “Full Size Cristal Can Relays”) с двумя переключающими контактами (два нормально замкнутых контакта используются для повышения надежности) коммутирующими ток 2 – 5 А, с обмоткой на 24 В постоянного тока. В качестве примера таких реле можно привести реле серий: РЭН33, РЭН34, РЭК134, РЭС48, 782XDXH, H782, B07, FW, SF, G2A-434ADC24, HGPRM-B4C05ZC, 2B-7506 и др.

Никакой особо точной настройки порога срабатывания этого устройства не требуется. Важно лишь, чтобы оно срабатывало всегда раньше МУРЗ, при любом подозрительном режиме в контролируемой цепи, поскольку излишние срабатывания устройства в результате неточной настройки не влияют на поведение защищаемого этим устройством МУРЗ.

Использование в предлагаемом устройстве высоконадежных компонентов, выбранных с многократными запасами по току, напряжению и мощности, допускающих работу в широком интервале температур, очень ограниченное количество этих компонентов, высокий уровень гальванической развязки, а также дублирование наиболее ответственных элементов позволяет обеспечить высокую надежность МУРЗ при воздействии мощных электромагнитных помех, кибератак и ПЭДВ, соответствующих надежности и устойчивости электромеханических реле.

Все элементы описанного устройства защиты должны быть размещены в отдельном корпусе и снабжены разъемами или клеммными колодками для подключения к МУРЗ.

Защищенные с помощью описанного устройства МУРЗ могут быть включены (при необходимости) и на параллельную работу для защиты особо ответственных объектов электроэнергетики. При использовании описанного устройства возможно также и включение параллельно МУРЗ дополнительных ЭМРЗ с задержкой на 0.1 сек [5.7].

Очевидно, что конкретные схемотехнические решения могут и отличаться от описанных в данной главе, однако предложенный подход к решению проблемы безусловно будет способствовать повышению надежности релейной защиты на основе МУРЗ.

Вне сомнения, найдутся такие специфические режимы работы релейной защиты и такие схемы взаимодействия между отдельны-

ми реле, для которых реализация предложенного метода защиты МУРЗ будет затруднительна. Это вполне естественно и ожидаемо. В таких специфических случаях может потребоваться или доработка предложенного метода, или изменение известных схем взаимодействия между реле. Описанное схемотехническое решение призвано лишь подтвердить техническую возможность реализации идеи защиты МУРЗ от ПДДВ помощью аппаратных, а не программных средств и может служить некоей отправной точкой для конкретных разработок устройства, пригодного для промышленного производства.

Дальнейшие усилия должны быть направлены на разработку конструкций входных реле на герконах (датчиков тока и напряжения) с регулируемым порогом срабатывания.

5.2. Датчики тока и напряжения на базе герконовых реле с регулируемым порогом срабатывания

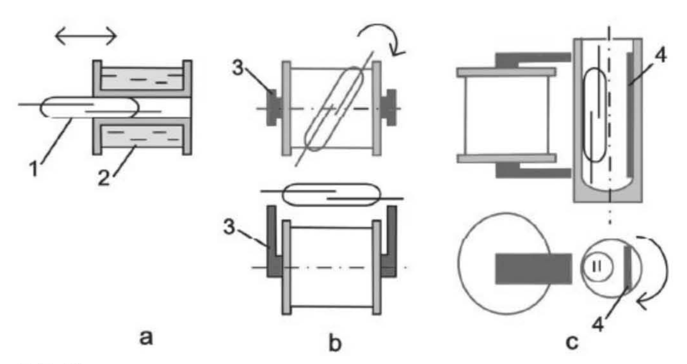


Рис. 5.5. Конструктивные схемы герконовых реле с регулируемым порогом срабатывания: **a** – с соосным перемещением геркона внутри катушки; **b** – с поворотом оси геркона относительно оси катушки и внешним расположение геркона; **c** – с эксцентричным перемещением геркона и магнитного шунта. 1 - геркон; 2 – катушка с обмоткой; 3 – ферромагнитный сердечник; 4 – ферромагнитная экранирующая пластина (магнитный шунт)

Герконовые реле – широко распространенные в технике компоненты, выпускаемые многими компаниями.

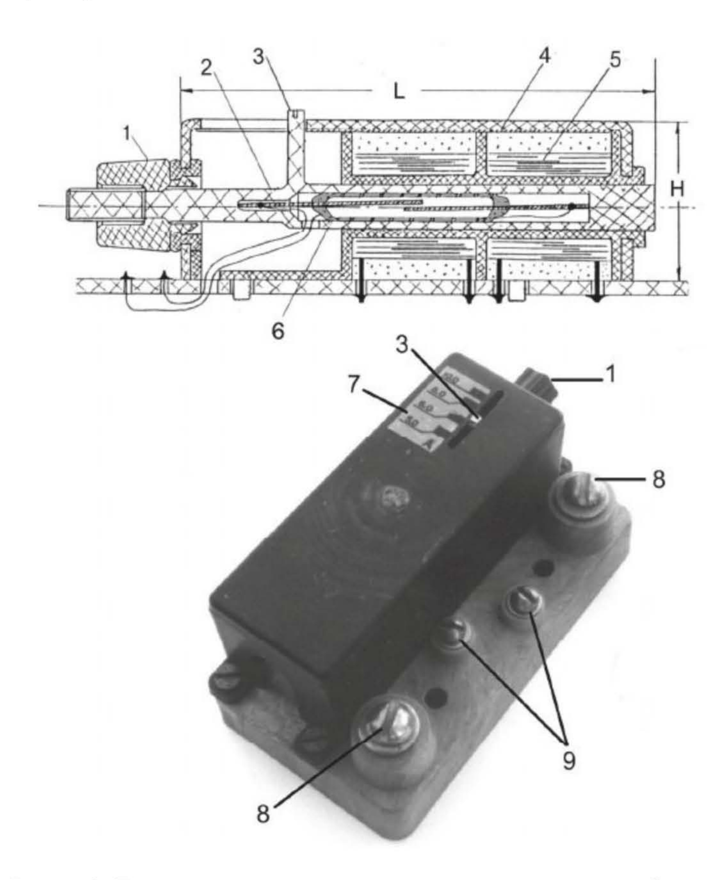


Рис. 5.6. Герконовое реле с регулируемым порогом срабатывания с аксиальным расположением геркона и катушки и с соосным перемещением геркона. 1 – вращающаяся ручка настройки; 2 – пластмассовая перемещающаяся деталь с запрессованным в нее герконом; 3 – указатель положения геркона; 4 – ферромагнитный экран; 5 – катушка с обмоткой; 6 – геркон; 7 – шкала; 8 – выводы обмотки; 9 – выводы геркона

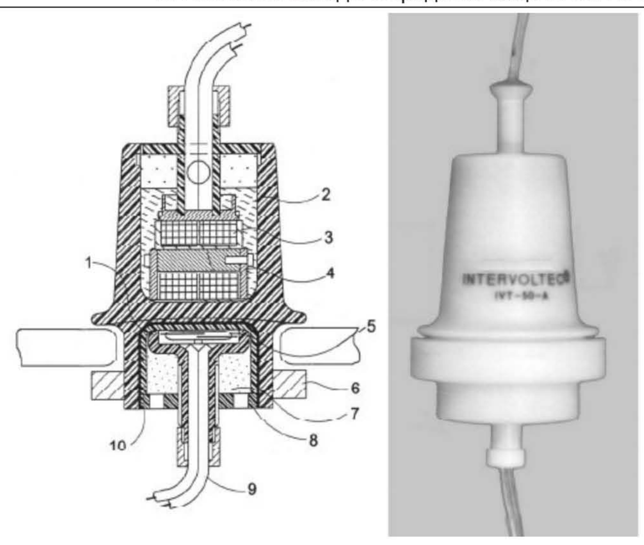


Рис. 5.7. Герконовое реле с регулируемым порогом срабатывания, реализованного по конструктивной схеме b с герконом, расположенным вне катушки, продольная ось которого образует угол с продольной осью катушки. 1 – пластмассовая капсула грибообразной формы с гнездом для геркона; 2 – заливочный эпоксидный компаунд полости корпуса с катушкой; 3 – катушка; 4 – ферромагнитный сердечник; 5 – геркон; 6 – гайка; 7 - заливочный эпоксидный компаунд поворотного корпуса с герконом; 8 – гайка-фиксатор поворотного корпуса; 9 – выводы геркона; 10 – поворотный корпус геркона

Такие преимущества герконов, как герметичность, высокий срок службы, высокое быстродействие, специальная газовая среда или вакуум в которых находятся контакт-детали, отсутствие необходимости в регулировке и зачистке контактов, высокий уровень гальванической развязки между входом (катушка управления) и выходом (герконом), четкий и стабильный порог срабатывания делают их незаменимыми в целом ряде систем автоматики и измерительной техники.

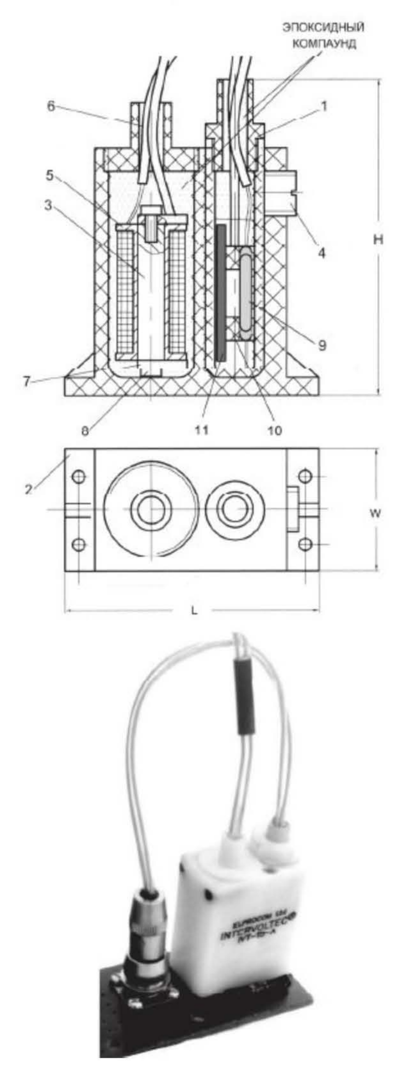


Рис. 5.8. Конструкция компактного реле с регулируемым порогом срабатывания, выполненного по схеме с эксцентричным перемещением геркона. 1 – выступающая часть поворотного корпуса-ампулы; 2 – крепежные фланцы; 3 – ферромагнитный сердечник; 4 – винт-фиксатор; 5 – катушка с обмоткой; 6 – выводы катушки; 7 – полюса сердечника; 8 – винты крепления полюсов; 9 – геркон; 10 – изоляционные проставки; 11 – магнитный шунт

Однако, ни одно из выпускаемых промышленностью герконовых реле не обладает возможностью регулирования порога срабатывания, что потребовало разработки конструкций таких реле.

Рассмотрим наиболее приемлемые для указанного применения конструктивные схемы герконовых реле с регулируемым порогом срабатывания, рис. 5.5.

Наиболее простым вариантом представляется конструктивная схема, приведенная на рис. 5.5а с соосным расположением геркона и катушки управления и с поступательным перемещением геркона вдоль оси катушки. Максимальной чувствительностью реле обладает, когда межконтактный зазор геркона располагается в центре катушки.

При смещении этого зазора относительно центра катушки чувствительность геркона к току, протекающему по катушке, снижается. Однако, практическая реализация этой конструктивной схемы оказалась не очень простой рис. 5.6.

Для перемещения геркона потребовалось изготовление узла, аналогичного червячному редуктору, в котором вращение вокруг своей оси ручки 1 с резьбой внутри приводит к перемещению винта с наружной резьбой, расположенного на конце детали 2 с запрессованным в ней герконом. Помимо сложности, недостатком конструкции является большая длина L реле, превышающая тройную длину колбы геркона. Еще одним недостатком конструкции является выход геркона из зоны эффективного магнитного экранирования при выдвижении геркона из катушки. Электрическая прочность изоляции между катушкой и герконом в этой конструкции не превышает 1 кВ.

Более простой с точки зрения реализации является конструктивная схема, представленная на рис. 5.6. В реле, построенном по этой конструктивной схеме, внутри катушки расположен ферромагнитный сердечник с полюсами, а геркон расположен на внешней стороне катушки с осью, параллельной оси катушки.

Конструктивная реализация реле, выполненного по этой схеме менее сложна, чем предыдущего, рис. 5.7

В положении, показанном на рис. 5.7, чувствительность реле максимальна. Загрубление реле осуществляется путем поворота геркона таким образом, чтобы между продольными осями катушки и геркона образовался угол. Минимальная чувствительность реле обеспечивается при угле в 90 градусов между упомянутыми осями.

В этой конструкции регулирование порога срабатывания осуществляется путем поворота в пределах 0 – 90 градусов корпуса 10 с помощью выходящего наружу конца капсулы с герконом и последующей фиксацией его положения гайкой-фиксатором 8. Крепление реле к внешней панели может осуществляться либо с помощью гайки 6 (как показано на рис. 5.7) или с помощью выступающего фланца с отверстиями и обычных винтов. Реле этого типа имеет корпус цилиндрической формы довольно большого диаметра (превышающего длину колбы геркона) и высоту, эквивалентную, примерно, тройной длине геркона. Электрическая прочность изоляции между герконом и катушкой в реле этой конструкции значительно

превышает уровень предыдущего реле и может достигать десятков киловольт. Достаточно указать, что такая конструкция была реализована автором для напряжений до 70 кВ (при соответствующей толщине изоляционного корпуса, его длине и выборе соответствующего изоляционного материала для его изготовления).

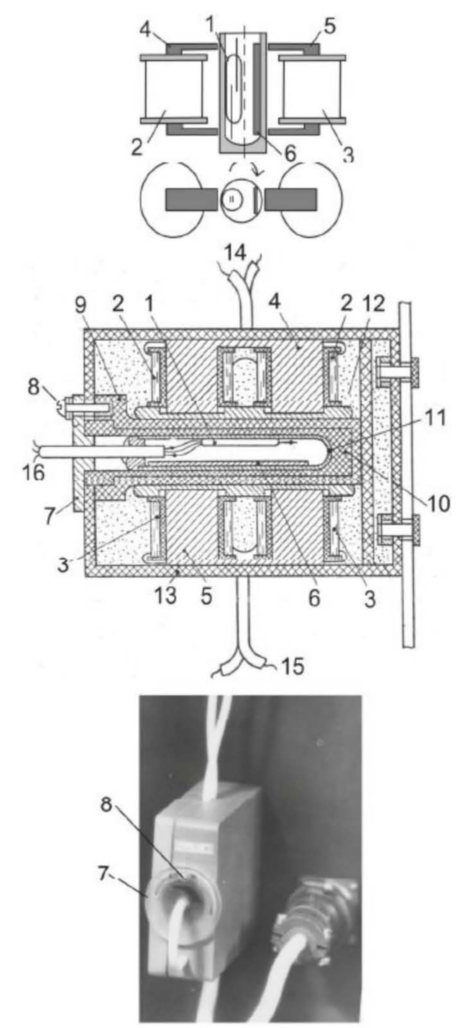


Рис. 5.9. Дифференциальное герконовое реле с регулируемым порогом срабатывания. 1 – геркон; 2 и 3 – катушки с обмотками управления; 4 и 5 – плоские ферромагнитные сердечники П-образной формы; 6 – магнитный шунт; 7 – лимб настройки реле; 8 – фиксатор лимба; 9 – неподвижный изолятор; 10 – поворотная часть изолятора; 11 – ампула с герконом и магнитным шунтом; 12 – заливочный эпоксидный компаунд; 13 – пластмассовый корпус реле прямоугольной формы; 14 и 15 – выводы обмоток управления; 16 – выводы геркона

Наиболее компактным является реле с регулируемым порогом срабатывания, реализованное по конструктивной схеме, показанной на рис. 5.5c. В этом реле геркон и магнитный шунт установлены напротив друг друга эксцентрично внутри поворотной ампулы.

В положении максимальной чувствительности геркон должен быть максимально приближен к полюсам сердечника обмотки управления, а магнитный шунт – максимально удален. При повороте упомянутой ампулы геркон удаляется от полюсов сердечника, а его место занимает магнитный шунт, ослабляющий магнитный поток в области геркона. Применение этого магнитного шунта позволило получить большой диапазон регулирования порога срабатывания геркона при малом диаметре поворотной ампулы, то есть позволило уменьшить размеры реле.

После настройки реле на выбранный ток срабатывания положение ампулы фиксируется с помощью винта 4. Это реле также обладает высокой электрической прочностью изоляции между герконом и катушкой управления, особенно при использовании проводов в высоковольтной изоляции в качестве выводов катушки и геркона.

С регулируемым порогом срабатывания может быть реализовано и дифференциальное реле, реагирующее на разность значений тока или напряжения, подведенных к двум разным входам этого реле, рис. 5.9.

Конструктивная схема этого реле, по сути, является разновидностью **c** (рис. 5.5), но отличается наличием двух катушек, расположенных в одной плоскости с противоположных сторон поворотной ампулы с герконом и магнитным шунтом.

В этой конструкции при повороте лимба изменяется взаимное расположение геркона 1 и магнитного шунта 6 относительно полюсов сердечников 4 и 5 катушек управления. В процессе поворота лимба геркон удаляется от одной катушки и приближается к другой, в результате чего изменяется степень влияния этих катушек (то есть входных сигналов) на геркон. Если полярность включения катушек выбрать противоположной, то в среднем нейтральном положении поворотного изолятора 10 напряженность магнитного поля в области геркона будет близка к нулю. При повороте изолятора с герконом, влияние одной катушки на геркон будет возрастать, а другой – ослабевать.

Конструкция этого реле обеспечивает высокий уровень гальванической развязки между входами и выходом за счет наличия высоковольтного изолятора 9. Если отливать этот изолятор заодно с корпусом из высококачественной пластмассы, а после сборки реле использовать заливку качественным эпоксидным компаундом под вакуумом, то можно достичь электрической прочности изоляции и этой конструкции в десятки киловольт.

Для совместной работы с микропроцессорными реле защиты (как об этом говорится в начале главы) изоляция в десятки киловольт является, разумеется, излишней. Но изоляция в 5-10 киловольт импульсного напряжения отнюдь не помешает, когда речь идет об устройстве защиты от воздействия мощного электромагнитного импульса, характеризующегося, как известно, высокими наведенными напряжениями. В конструкциях по схемам **b** и **c** такой уровень изоляции реализуется без всяких проблем, поскольку эти конструкции изначально были разработаны именно для работы при высоких напряжениях [5.9].

Описанные конструкции были проверены на практике и показали отличные характеристики и как реле максимального напряжения и как реле максимального тока. Однако, в некоторых практических случаях, например, когда речь идет об их применении в устройствах защиты микропроцессорных реле, реализующих функцию дистанционной защиты, может потребоваться реле минимального напряжения.

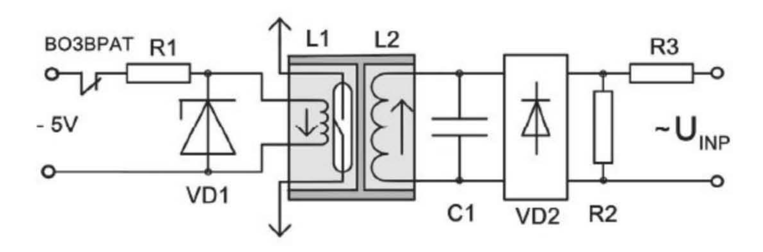


Рис. 5.10. Герконовое реле минимального напряжения

Для реализации функции реле минимального напряжения непосредственно на герконе должна быть размещена дополнительная

обмотка L1 с относительно небольшим числом витков, которая в схеме подключается к стабилизированному источнику напряжения 5 В, а изолированная от геркона рабочая обмотка L2 подключена через диодный выпрямитель VD2 и сглаживающий конденсатор C1 пленочного типа, рис. 5.10, обладающих очень большими запасами по напряжению (входное напряжение со стандартного трансформатора напряжения, применяемого в электроэнергетике обычно не превышает 100 В).

Обмотки L1 и L2 включены встречно, таким образом, что суммарное магнитное поле в области геркона близко к нулю в нормальном рабочем режиме. При значительном снижении входного напряжения (на которое, одновременно с увеличением тока обычно реагирует дистанционная защита линий электропередач) магнитное поле обмотки L2 ослабевает, а магнитное поле, создаваемое обмоткой L1, остается неизменным. Результирующее магнитное поле в области геркона возрастает и он срабатывает. Конструкция самого герконового реле может быть любой из рассмотренных выше.

В устройстве могут быть использованы диоды типа BY 2000 (Diotec Semiconductor) на напряжение 2000 В и ток 3 А (импульсный ток 80 А) в корпусе типа DO-201 (диаметр 4.5 мм, длина 7.5 мм). Конденсатор типа MKP1T041007H00 (WIMA) 1 мкф, 1600 В, имеющий размеры: 24 х 45.5 х 41.5 мм. Эти элементы размещены на печатной плате устройства вне корпуса реле. Использование таких высоковольтных элементов при сравнительно низком напряжении, поступающем на схему после делителя на резисторах R2-R3 (15 – 20 В) необходимо для обеспечения высокой стойкости устройства к перенапряжениям, генерируемым мощным электромагнитным импульсом.

Во всех описанных выше реле рекомендуется использовать миниатюрные вакуумные герконы, выдерживающие испытательное напряжение не менее 1 кВ и имеющие собственное время срабатывания около 1 мс, табл. 5.1

Изоляционные элементы конструкции всех рассмотренных типов реле рекомендуется выполнять из литьевого термопластика типа ULTEM-1000 (Polyetherimide – PEI) – полупрозрачного материала янтарного цвета обладающего отличной совокупностью механических, температурных (-55 +170 ºC) и электрических (33 кВ/мм, $tg\delta = 0.0012$) свойств, малой водопоглощаемостью (0.25% за 24 ча-

са), высокой стойкостью к излучениям различных типов, относительно хорошей адгезией к эпоксидным компаундам. А в качестве заливочного эпоксидного компаунда – STYCAST 2651-40 (Emerson & Cumming) – двухкомпонентный компаунд черного цвета, обладающий хорошими диэлектрическими свойствами (18 кВ/мм, tgδ = 0.02), малой водопоглощаемостью (0.1 % за 24 часа), широким интервалом рабочих температур (-75 +175 ºC) очень низкой вязкостью в жидком состоянии и хорошей адгезией к металлам и пластикам. Этот компаунд имеет близкий к ULTEM-1000 коэффициент линейного расширения, что немаловажно при работе реле в широком интервале температур. В качестве отвердителя должен применяться CATALYST-11.

Следует иметь ввиду, что заливать геркон непосредственно эпоксидным компаундом нельзя. Его нужно предварительно покрыть слоем демпфирующего материала, компенсирующего механические напряжения, возникающие в процессе отверждения эпоксидного компаунда.

Для предотвращения проникновения высокочастотных и импульсных помех в выходные цепи реле через его емкость, геркон помещен в заземленную тонкостенную алюминиевую ампулу.

Рассмотренные технические решения могут послужить практической основой при подготовке производства реле тока и напряжения с регулируемым порогом срабатывания для устройств, предназначенных для повышения устойчивости микропроцессорных реле защиты к кибератакам и преднамеренным дистанционным деструктивным воздействиям.

5.3. Технико-экономические аспекты метода активной защиты микропроцессорных реле

В выше была показана уязвимость микропроцессорных устройств релейной защиты (МУРЗ) к преднамеренным дистанционным деструктивным воздействиям - ПДДВ (электромагнитным и кибернетическим), обоснована необходимость защиты МУРЗ и описан конкретный метод защиты, основанный на совместном использовании МУРЗ и пускового органа на герконах, функционально включенного последовательно с МУРЗ и деблокирующего его только в том случае, когда хотя бы один из контролируемых пара-

метров (ток, напряжение, угол между ними и т.д.) приближается к порогу срабатывания МУРЗ, рис. 5.1.

Сама постановка проблемы, а также предлагаемый метод защиты МУРЗ от ПДДВ настолько необычны и настолько отличаются от всего того, что было известно ранее, что неизбежно вызывают у специалистов море вопросов и шквал эмоций (увы, не всегда положительных). Отсутствие ответов в статьях, опубликованных ранее, на многие из возникающих вопросов, часто приводит к непониманию, а отсюда и к полному неприятию предлагаемого метода. Поэтому попробуем сформулировать наиболее часто задаваемые в дискуссиях на эту тему вопросы и дать на них ответы.

Вопрос 1. Судя по схеме, герконы навешиваются на МУРЗ со всех сторон, как гирлянды на елку?

Совершенно очевидно, что герконы не «навешиваются как гирлянды» на входы и выходы МУРЗ, а вместе со всеми остальными элементами предлагаемого устройства защиты располагаются внутри отдельного экранированного корпуса, аналогичного по конструкции корпусам МУРЗ с той лишь разницей, что в нем нет необходимость в экране, но имеется доступ к узлам регулирования порога срабатывания герконовых реле порогового органа. Этот отдельный модуль снабжен такими же клеммными колодками для присоединения к внешним цепям, как и МУРЗ.

Вопрос 2. В отношении герконов имеется распространенное мнение об их ненадежности (залипании). Насколько оправдано их применение в устройстве, которое должно обладать повышенной надежностью?

Герконы, вернее реле на основе герконов, используемые в пусковом органе устройства защиты (ПОУЗ), отличаются от обычных электромеханических реле целым рядом положительных качеств. Во-первых, контакт-детали сухих герконов находятся в герметичном баллоне, заполненном смесью инертных газов под давлением или вакууммированного и поэтому они не подвержены влиянию отрицательных факторов внешней среды (влаги, пыли, газов). Эти контакты не требуют регулировки и зачистки в течение всего срока службы. Во-вторых, реле на герконах имеют быстродействие в 3-5 и более раз превышающее быстродействие обычных электромехани-

ческих реле. В-третьих, на переменном токе герконовые реле имеют коэффициент возврата 0.9 – 0.95, что намного превышает аналогичный параметр обычных реле. В-четвертых, в герконовых реле можно простыми средствами достичь уровня гальванической развязки входа от выхода (катушки от контактов) в десятки киловольт, что недостижимо для обычных электромеханических реле. В-пятых, в отличие от обычных реле, герконовые реле имеют четкий и стабильный порог срабатывания при плавном увеличении тока в катушке управления, что позволяет создавать на основе герконов чувствительные измерительные органы защит. В дополнение в вышесказанному можно отметить, что сухие герконы нечувствительны к положению в пространстве и хорошо сочетаются с электронными, электромагнитными и магнитными элементами, что позволяет создавать на их основе множество различных функциональных модулей и устройств [5.10].

Высококачественные вакуумные и газонаполненные герконы, производимые ведущими компаниями, специализирующимися в этой области (а именно такие предполагается использовать в устройстве [5.11]), являются не дешевыми (15 – 30 долларов за штуку), но высоконадежными компонентами, нашедшими широкое применение не только в промышленности и технике связи, но и в военной и аэрокосмической технике. Герконы по многим своим параметрам занимают промежуточное положение между полупроводниковыми и электромеханическими коммутационными элементами. Поэтому автоматические телефонные станции – АТС на основе герконов (типа «Квант» и др.) называются «квазиэлектронными». По техническим условиям срок службы таких АТС установлен в 40 лет, причем количество отказавших за это время герконов не должно превышать 0.3%. Уже одни только эти цифры говорят сами за себя.

Однако у герконовых реле имеется одно принципиальное отличие от обычных электромеханических реле: их магнитная система не изолирована от контактов, а образована самими контактами. Это отличие обуславливает низкую перегрузочную способность герконов по току. В отличие от обычных реле, герконовые реле не допускают даже кратковременной токовой перегрузки контактов. Причиной этого является тот факт, что магнитное поле тока, проходящего через замкнутые контакты геркона направлено встречно магнитному полю обмотки, удерживающему контакты в замкнутом состоя-

нии и ослабляет его, ослабляя контактное нажатие, вплоть до образования зазора. Это приводит к усиленной эрозии, а иногда и к свариванию контактов геркона даже при кратковременном протекании тока, превышающего максимально допустимое для данного типа значение. Незнание этой особенности герконов и их использование без учета отличий от обычных реле в части перегрузочной способности часто приводит к отказам оборудования и, как следствие, к недоверию к герконам. При правильно выбранном режиме работы герконов они обеспечивают надежную коммутацию цепей при миллионах циклов срабатывания. При использовании герконов для коммутации внешних цепей, ток в которых может изменяться в широких пределах, никто не хочет следить за токовым режимом работы герконов. Гораздо проще отказаться от их использования, что часто и происходит на практике. В предложенной конструкции часть герконов включены лишь во внутренние цепи устройства, токовая нагрузка в которых в десятки раз меньше максимально допустимой для герконов. Другая часть отключает цепи дискретных входов, токи в которых не превышают нескольких миллиампер, что на два порядка меньше предельно допустимого значения. И только через герконы, включенные последовательно с выходными контактами МУРЗ, предназначенными для включения отключающей катушки выключателя, могут проходить токи в несколько ампер. Однако, во-первых, эти герконы непосредственно не осуществляют коммутацию этих токов, а лишь собирают цепь без тока, а во-вторых, они выбраны такого типа (Bestact R15U, производства японской компании Yaskawa), который обеспечивает большие запасы по току.

Вопрос 3. Современные МУРЗ совмещают 10-20 и более различных функций в одном терминале. Значит ли это, что предлагаемое устройство защиты должно содержать такое же количество входных реле?

Нет, не значит. Дело в том, что все многообразие реализуемых сегодня в одном терминале МУРЗ функций основано на измерениях тока, напряжения и угла между ними. Соответственно и входные реле предлагаемого устройства защиты должны содержать пороговые элементы тока, напряжения и угла между ними. Пороги сраба-

тывания всех этих элементов должны быть меньше минимальных значений, выбранных в качестве уставки МУРЗ.

Вопрос 4. Зачем нужно применять дорогие МУРЗ совместно с какими-то новыми и тоже дорогими устройства защиты, если можно просто вернуться к использованию дешевых и устойчивых к ПДДВ электромеханических реле защиты?

Действительно, электромеханические реле защиты (ЭМРЗ) эксплуатируются уже более ста лет и до сих пор обеспечивают надежную защиту от аварийных режимов всех видов электрооборудования.

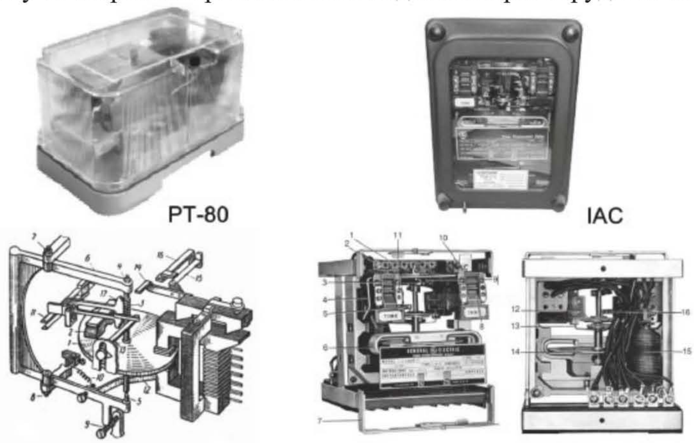


Рис. 5.11. Внешний вид и устройство аналогичных по параметрам и конструкции электромеханических реле тока с зависимой выдержкой времени: слева РТ-80 производства Чебоксарского завода ЧЭАЗ, справа IAC производства General Electric

Достаточно сказать, что такая большая и разветвленная национальная энергосистема, как российская, даже сегодня почти на 90% укомплектована ЭМРЗ. Однако, несмотря на то, что ЭМРЗ доказали свою высокую надежность, примерно 30-40 лет тому назад все ведущие мировые производители реле защиты перестали заниматься разработкой и совершенствованием ЭМРЗ и начали интенсивно разрабатывать сначала полупроводниковые реле, полностью копирующие функции и характеристики ЭМЗ, а затем и микропроцес-

сорные реле защиты, копирующие функции полупроводниковых реле, рис. 1.10. Лишь спустя годы на рынке появились микропроцессорные реле с расширенным набором функций и улучшенными характеристиками.

Примерно 20-25 лет тому назад большинство ведущих мировых производителей РЗ просто перестали выпускать ЭМРЗ, сосредоточив все свои усилия на МУРЗ. Основная причина этого явления заключается в том, что производить на автоматическом оборудовании печатные платы с электронными элементами и затем тестировать их также на автоматическом оборудовании, значительно выгоднее, чем изготавливать на высокоточных токарных и фрезерных станках миниатюрные элементы, вручную собирать из них достаточно сложную механическую конструкцию, вручную тестировать и настраивать.

Ввиду большой разницы в себестоимости производства между ЭМРЗ и МУРЗ, потребитель тоже оказывается в выигрыше, поскольку стоимость МУРЗ, производимых мировыми лидерами релестроения сегодня уже намного меньше стоимости аналогичного по характеристикам ЭМРЗ. Утверждение, что ЭМРЗ сегодня значительно дешевле МУРЗ в большинстве случаев не корректно и не подтверждается анализом цен на мировом рынке. Так, например, если электромеханическое реле трехступенчатой дистанционной защиты линий типа LZ31 (производства ABB) по нынешним ценам стоило бы порядка 30-35 тысяч долларов США, то его микропроцессорный аналог с улучшенными характеристиками – реле типа D30 (General Electric) стоит сегодня всего лишь 7.000 долларов США, а китайский аналог типа GTL-823 (Guatong Electric) и того меньше – 4.5 тыс. долларов.

Что касается цен на рынке стран постсоветского пространства, то они сильно искажены и не соответствуют соотношению цен, существующему на мировом рынке. Например, если сравнить цены на близкие по конструкции и характеристикам электромеханические реле тока с зависимой характеристикой: российские РТ-80 и американские IAC (рис. 5.11), то окажется, что реле российского производства (около 60 долларов США) стоят более чем в 20 раз дешевле американского IAC (около 1400 долларов США).

Такую разницу в ценах можно было бы объяснить использованием в России более дешевого оборудования, более дешевых мате-

риалов, а главное более дешевой рабочей силы. Но тогда следовало бы ожидать, что и соотношение стоимостей МУРЗ российского и западного производства будет пусть не точно такой же, но хотя бы близкой. Что же мы видим на практике? Возьмем в качестве примера реле дистанционной защиты линий: уже упомянутое реле D30 (General Electric) и аналогичное по параметрам реле Сириус-3-ЛВ-03 (НПП Радиус Автоматика), рис. 5.12. Оказывается, что их стоимости примерно равны (6500 – 7000 долларов США). Чем это можно объяснить, с учетом вышесказанного? Даже если принять во внимание, что в российских МУРЗ применяется много электронных компонентов западного производства, все равно будет трудно объяснить объективными причинами такое странное соотношение цен. Скорее всего, здесь имеет место явное завышение цен российскими производителями МУРЗ с целью получения сверхприбыли.

Рис. 5.12. Микропроцессорное реле дистанционной защиты линий D30 (производства GE, США) и Сириус-3-ЛВ-03 (производства НПП «Радиус-Автоматика, Россия), имеющие схожие характеристики и стоимость

Если ориентироваться на существующее в России искаженное ценообразование то, скорее всего, с практическим применением предложенного устройства защиты действительно могут возникнуть существенные трудности.

С другой стороны, мощнейшая рекламная компания, организованная производителями, разработчиками МУРЗ, университетами и исследовательскими организациями, заинтересованными в финансировании новых проектов, сделали свое дело. Сегодня поднять вопрос о возврате к ЭМРЗ - означает стать изгоем в сообществе специалистов и прослыть ретроградом, пытающемся остановить тех-

нический прогресс. Никто из специалистов или чиновников, от которых зависит принятие решения, не возьмет на себя такую ответственность. А если и возьмет, то с уверенностью можно утверждать, что в этом случае на него обрушится бурный поток обвинений в ретроградстве и некомпетентности. Кроме того, объективности ради нужно отметить, что МУРЗ действительно обладают некоторыми характеристиками и функциональными возможностями, недоступными для ЭМРЗ.

С учетом всех этих факторов можно констатировать, что вопрос о возврате к ЭМРЗ на повестке дня не стоит, даже если при существующем в России соотношении цен он оправдан с экономической точки зрения.

Вопрос 5. Допустим, что возврат к ЭМРЗ сегодня уже действительно не возможен. Но тогда почему бы не использовать МУРЗ в комплекте с этими ЭМРЗ вместо того, чтобы изобретать какие-то новые устройства на герконах?

На самом деле, совместное применение МУРЗ и ЭМРЗ уже давно используется на практике, рис. 5.13. Правда, не в последовательном соединении, как предложено нами, а в параллельном, то есть для дублирования друг друга с целью повышения надежности. Как показано нами ранее [5.7], такой метод использования МУРЗ и ЭМРЗ (то есть, их параллельное соединение) неверен по своей сути. При использовании такого параллельного включения ЭМРЗ действительно должны полностью повторять функции МУРЗ и иметь такие же установки. В любом случае совместного использования многофункционального МУРЗ и ЭМРЗ потребуется целый набор совсем не дешевых ЭМРЗ, что делает такой проект весьма сомнительным из-за его высокой стоимости и необходимости в больших площадях для монтажа большого количества различных ЭМРЗ.

Рис. 5.13. Фрагмент панели дистанционной защиты ответственных линий 160 кВ, содержащей электромеханические реле типа LZ31 (вверху), включенные на параллельную работу с микропроцессорными защитами типа MiCOM P437 (внизу)

Предложенное устройство защиты на базе герконовых реле должно быть намного проще, меньше и дешевле комплекта ЭМРЗ необходимого для защиты одного МУРЗ. Только в этом случае оно может иметь перспективы применения.

Вопрос 6. Предложенное устройство защиты чтобы быть универсальным и полноценно работать, по своим функциональным возможностям должно быть таким же, как набор ЭМРЗ. Значит, стоимость его должна быть примерно такая же. Почему оно будет дешевле?

Давайте рассмотрим, как работает ЭМРЗ. Возьмем, например, электромеханическое токовое реле с зависимой выдержкой времени, в котором при достижении некоторого порогового уровня тока алюминиевый диск начинает медленно поворачиваться, а подвижный контакт, связанный с этим диском, приближаться к неподвижному (реле типа IAC, рис. 5.11). Через некоторое время, обуслов-

ленное скоростью вращения диска (которая определяется величиной тока, протекающего через катушку реле), контакт замкнет (через промежуточное реле) цепь отключающей катушки выключателя. Для пускового органа предлагаемого устройства защиты МУРЗ никакой выдержки времени, зависящей от тока не требуется. Этот пусковой орган должен лишь сработать при определенной величине тока, несколько меньшей тока трогания упомянутого диска. И все. Больше никаких других функций от него не требуется, поскольку все остальные функции будет осуществлять активированный МУРЗ.

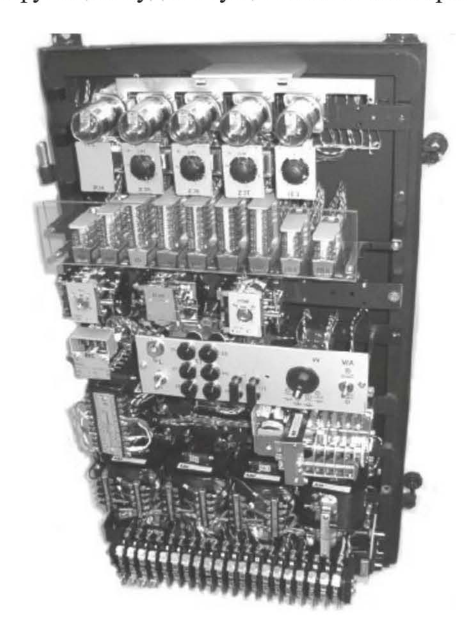


Рис. 5.14. Реле дистанционной защиты линий LZ31

То есть в данном случае вместо сложного и дорогого реле с зависимой выдержкой времени используется простейшее реле, содержащее катушку и геркон.

В качестве другого примера рассмотрим несколько типов реле дистанционной защиты линий.

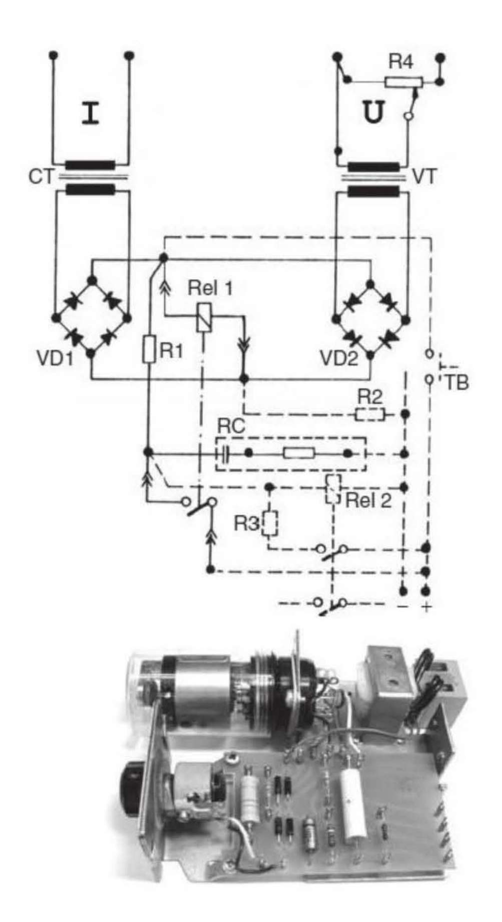


Рис. 5.15. Принцип действия и конструкция пускового органа реле дистанционной защиты типа LZ31

Электромеханический вариант этого реле, например, типа LZ 31, рис. 5.14, содержит множество сложных взаимосвязанных между собой электромеханических узлов, обеспечивающих три ступени измерения сопротивления линии до места короткого замыкания, соответствующие этим ступеням выдержки времени, особой формы характеристику и т.д. Как уже отмечалось выше, стоимость такого реле составляет 30-35 тыс. долларов.

Вместе с тем, пуск всего этого комплекса осуществляется простейшим пусковым органом, осуществляющим контроль баланса между током и напряжением линии, рис. 5.16. Срабатывание этого органа осуществляется при нарушении баланса между током и напряжением.

В довольно сложных и крупных реле х дистанционной защиты типов RYZKB, RYZOE, RYZFB, производимых компанией ASEA в 70-х годах, рис. 5.16, реализуются несколько защитных функций. Однако, все эти реле имеют в своем составе очень простой пусковой орган, схема которого показана на рис. 5.16. Эти пусковые органы являлись интегральной частью сложных конструкций и отдельно не выпускались. Исключение составляют некоторые типы реле, выпускавшиеся ЧЭАЗ, например, реле типа КРС-112, рис. 5.17, содержащее специальные дроссели и четырехполюсный индукционный механизм с вращающимся ротором. Это реле является, по-существу, отдельным пусковым органом дистанционных защит.

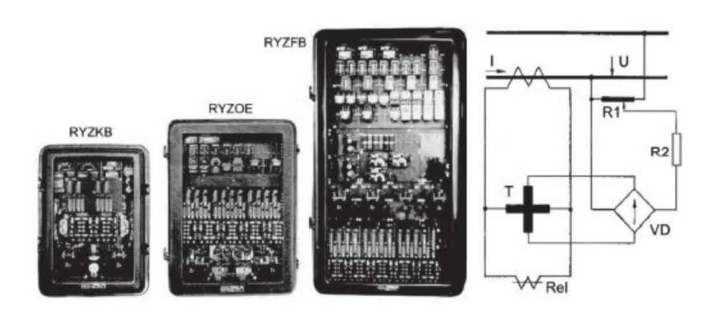


Рис. 5.16. Электромеханические реле дистанционной защиты различного типа фирмы ASEA и схема их пускового органа (производство 70-х годов)

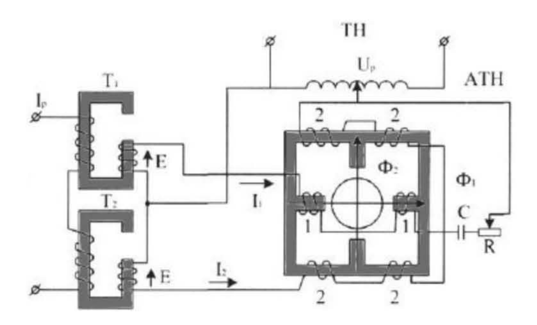


Рис. 5.17. Реле КРС-112 с индукционным механизмом

Однако, и оно слишком сложно, дорого и имеет большие габариты. Да и вообще, применение давно уже морально устаревшей конструкции в сочетании с самыми современными технологиями МУРЗ, вряд ли можно назвать удачной идеей.

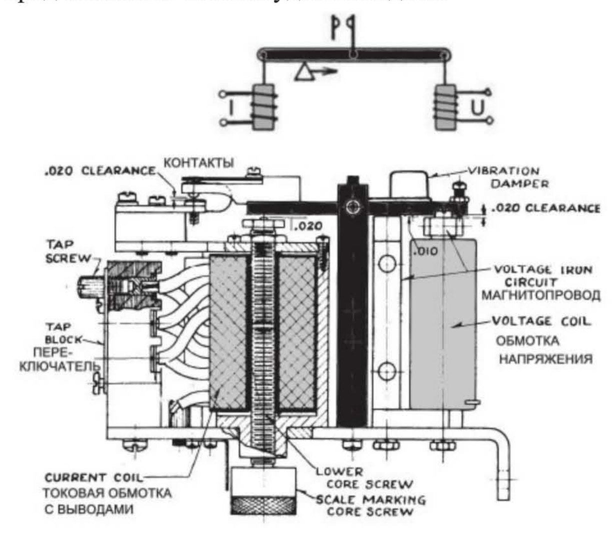


Рис. 5.18. Электромагнитный пусковой орган балансового типа, используемый в реле дистанционной защиты типа HZM (Westinghouse)

В этом отношении гораздо более привлекательным мог бы быть пусковой орган дистанционной защиты типа HZM (Westinghouse), рис. 5.18. Это очень простое устройство, содержащее Т-образный сердечник с качающимся коромыслом (верхняя часть буквы Т) и две катушки: тока и напряжения, воздействующих на концы коромысла. Положение этого коромысла, с прикрепленным к нему контактом, зависит от баланса магнитных полей, создаваемых катушками тока и напряжения. Этот узел является внутренней частью конструкции реле HZM и отдельно никогда не выпускался.

Герконовое реле, построенное по такому же принципу баланса между током и напряжением (рис. 5.19), получается намного проще и надежнее [5.11].

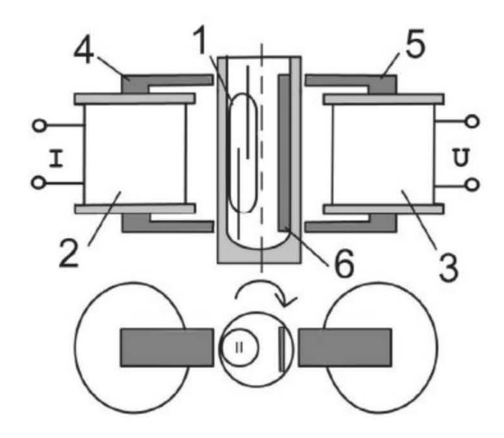


Рис. 5.19. Простейший пусковой орган дистанционной защиты с регулируемым порогом срабатывания. 1 – геркон; 2 и 3 – катушки с обмотками управления; 4 и 5 – плоские ферромагнитные сердечники П-образной формы; 6 – магнитный шунт

Это реле реагирует на разность магнитных полей, образованных катушками тока и напряжения и его порог срабатывания может регулироваться в широких пределах поворотом капсулы с герконом. Такой пусковой орган может быть с успехом использован в ПОУЗ.

Таким образом, предлагаемое устройство с небольшим количеством простейших (на базе герконов) пусковых органов тока, напряжения, разности между ними оказывается несравненно проще и дешевле, чем полнофункциональный комплект ЭМРЗ. Кроме того, пусковые органы на герконах не требуют обслуживания в процессе эксплуатации, привносят значительно меньшую задержку в общее время срабатывания РЗ, имеют высокий уровень изоляции входа от выхода, недостижимый для старых ЭМРЗ.

Вопрос 7. В некоторых случаях команды на отключение выключателей поступают напрямую от реле защит (например, таких как газовая защита трансформатора) и одновременно дублируются сигналами на дискретные входы МУРЗ, запуская, таким образом, регистратор аварийных событий. Как в таком случае будет работать предлагаемое устройство, блокирующее дискретные входы МУРЗ?

В этой ситуации все решается достаточно просто: необходимо лишь завести сигнал с контактов запускающего реле (в данном случае это газовое реле) еще и на один из входов ПОУЗ. При этом МУРЗ будет деблокировано и регистратор аварийных событий запустится и запишет информацию о срабатывании газового реле.

Вопрос 8. Известно требование о недопустимости введения в цепь отключающей катушки выключателя каких-то дополнительных блокирующих элементов, а в предложенном устройстве эта цепь разрывается контактом дополнительного реле. Разве такое допустимо?

На самом деле нормально разомкнутый контакт дополнительного реле включен не в цепь отключающей катушки выключателя, в цепь, соединяющую контакт выходного реле МУРЗ с отключающей катушкой выключателя. То есть этот дополнительный контакт блокирует не цепь отключающей катушки выключателя, а всего лишь выходную цепь МУРЗ. Цепь отключающей катушки выключателя остается свободной для подключения любых внешних контактов или ключей с ручным управлением.

Вопрос 9. Как быть со сложными защитами, например, с защитами, обеспечивающими отстройку от бросков тока намагничивания трансформатора и содержащих фильтры 2 и 5 гармоник? Предлагаемое устройство тоже должно содержать такие фильтры? Или другой пример: дифференциальная защита. Как обеспечить работу устройства при наличии аварийного режима только в защищаемой зоне?

Нет, для работы ПОУЗ не нужны такие фильтры и не нужна отстройка от броска тока намагничивания. Срабатывание ПОУЗ от броска тока намагничивания трансформатора лишь деблокирует МУРЗ на время около 10 секунд и не более того. Блокировка МУРЗ от излишних срабатываний обеспечивается его собственным алгоритмом. По истечении этих 10 секунд ПОУЗ возвращается в исходное состояние и опять блокирует МУРЗ. То же самое относится и к дифференциальной защите. Устройству ПОУЗ не важно где находится повреждение: в защищаемой зоне или вне ее. Для него важно лишь наличие тока КЗ, а зону повреждения будет определять МУРЗ после того, как ПОУЗ деблокирует его. Время срабатывания ПОУЗ составляет около 6 мс, что при собственном времени срабатывания МУРЗ 30-40 мс практически не влияет на общее время действия релейной защиты.

Вопрос 10. При последовательном включении ЭМРЗ и МУРЗ возможности релейной защиты фактически будут ограничены возможностями ЭМРЗ, как элемента, обладающего более скромными возможностями и худшими характеристиками. Хорошо ли это?

Нет, это не так. Предложенное устройство никоим образом не определяет ни свойства, ни характеристики релейной защиты. Оно лишь включает МУРЗ в работу в момент, когда хотя бы один параметр из всей совокупности контролируемых параметров приблизится к уставке МУРЗ. Дальнейшее поведение реле защиты и его реакция на аварийный режим будет определяться полностью свойствами и характеристиками этого реле.

На практике, очевидно, найдутся более сложные режимы работы МУРЗ, не рассмотренные в статье, для которых нужно будет разработать особый пусковой орган. Такая ситуация не исключена. Однако, даже если и потребуется создание такого специального

пускового органа, то на основе комбинации герконов и магнитных цепей возможно создание таких органов значительно более простых, дешевых и быстродействующих чем традиционные электромеханические реле защиты.

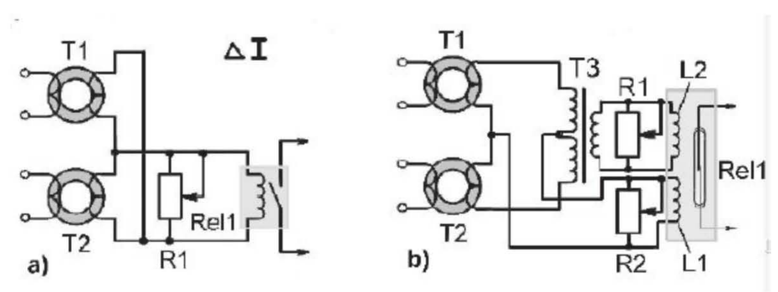


Рис. 5.20. Варианты квазиэлектронных пусковых органов дифференциальной защиты

Например, устройство, изображенное на рис. 5.20 может быть вполне использовано для контроля угла между током и напряжением или в качестве измерительного органа мощности.
Дополнительные возможности открываются при использовании комбинации магнитных и высоковольтных полупроводниковых элементов с герконами. Например, на рис. 5.20а показано простейшее устройство, реагирующее на разность токов, а на рис. 5.20в - с загрублением чувствительности к разностному току по величине прямого тока.

Вопрос 11. Высокочастотные и импульсные помехи могут проникать в МУРЗ и через цепи тока и напряжения. Как их защитить с помощью предложенного метода?

Вопрос о целесообразности защиты цепей тока и напряжения и конкретных технических решений, обеспечивающих такую защиту, требует дополнительного изучения. Дело в том, что входные токи и напряжения поступают на электронную схему МУРЗ через входные трансформаторы тока и напряжения, имеющиеся в каждом МУРЗ,

преобразующие достаточно мощные входные величины в маломощные сигналы. Эти сигналы представляют собой единицы вольт, поступающие на аналогово-цифровой преобразователь (АЦП), в котором аналоговые сигналы квантуются по уровню и преобразуются в цифровой код. Квантование (дискретизации) происходит в МУРЗ с достаточно низкой частотой 600 – 1200 Гц и поэтому весь процесс занимает некоторое время, на несколько порядков превышающее длительность импульсов ПЭДВ. За время действия импульса ПЭДВ АЦП просто не успеет произвести необходимые преобразования. Поэтому характер воздействия на МУРЗ импульсов ПЭДВ, проникших через цепи тока и напряжения будет определяться индуктивными и кондуктивными наводками, мало чем отличающимися от таких же наводок, проникших в МУРЗ другими путями. Однако, имеется и возможность существенного ослабления этих наводок, путем отключения и шунтирования вторичных цепей тока и напряжения упомянутых внутренних входных трансформаторов. Для этого эти цепи должны быть выведены на отдельный внешний соединитель производителем МУРЗ с тем, чтобы подключить через них герконы предлагаемого устройства защиты к этим цепям.

Таким образом, из проведенного анализа хорошо видно, что практическая реализация предложенного метода защиты МУРЗ с технической и экономической точки зрения вполне осуществима при условии отделения функций РЗ от всех остальных функций, которые навешиваются сегодня на МУРЗ, как гирлянды на елку. Такая реализация, безусловно, должна осуществляться предприятиями-производителями МУРЗ, которые могут предлагать потребителям квазиэлектронный ПОУЗ как дополнительную опцию для повышения безопасности и надежности работы релейной защиты ответственных объектов.

5.4. Защита системы дистанционного управления выключателями

Из-за негативной тенденции навешивания на МУРЗ всевозможных дополнительных функций, не имеющих отношения к релейной защите [5.12, 5.13], реализация предложенных выше мер защиты

МУРЗ в некоторых случаях будет затруднена. Речь идет о распространенном использовании МУРЗ для дистанционного управления выключателями (ДУВ). Совершенно очевидно, что такое использование МУРЗ не имеет ничего общего с функциями релейной защиты, а дистанционное подключение к МУРЗ по каналам связи с целью изменения положения выключателей очень трудно отличить аппаратными средствами от кибератаки.

Как нами уже было неоднократно показано ранее, задачу повышения надежности релейной защиты невозможно решить при совмещении функций МУРЗ с функциями, не имеющими отношения к РЗ, например таких популярных, как мониторинг исправности электрооборудования, дистанционное управление выключателями и т.п. МУРЗ должны использоваться исключительно для решения задач релейной защиты. Тем более, что для решения других задач, например, для мониторинга электрооборудования, сегодня на рынке имеется огромное количество специализированных устройств, от простейших реле, контролирующих целостность цепи отключающей катушки выключателя, до сложнейших комплексов, контролирующих в режиме реального времени состав газов, растворенных в масле трансформаторов или уровень частичных разрядов в изоляции. По нашему мнению, и ДУВ должно быть отделено от релейной защиты и осуществляться отдельными аппаратными средствами. Только в этом случае можно повысить надежность РЗ и осуществить ее эффективную защиту от преднамеренных дистанционных деструктивных воздействий. При таком разделении функций появляется возможность не только обеспечить высокоэффективную защиту МУРЗ, но и реализовать защищенную дистанционную систему управления выключателями (ЗДУВ).

Предлагаемая система ЗДУВ, рис. 5.21, является гибридной и совмещает в себе как микропроцессорный контроллер с сетевым каналом передачи данных, так и кабельный канал с электромеханическими реле. Основной задачей предлагаемой системы является предотвращение несанкционированных изменений положения выключателей при кибератаке или при повреждениях электронных устройств, входящих в эту систему. Вспомогательной задачей системы является повышение ее живучести и сохранение работоспособности после воздействия ПЭДВ. Общая идея такой системы заключается в том, что любая команда на изменение положения вы-

ключателя, передаваемая по сетевому каналу, должна быть подтверждена кратковременным дистанционным включением электромеханического реле на подстанции путем подачи напряжения на его катушку по обычному контрольному кабелю. Почему потребовалось использование электромеханического реле и почему нельзя использовать подтверждающий канал на основе волоконно-оптической линии связи (ВОЛС)?

Проблема заключается в том, что ВОЛС не решает задачи защиты от ПЭДВ, поскольку с двух сторон эти ВОЛС снабжены сложными микропроцессорными мультиплексорами, обеспечивающими преобразование электрических сигналов в световые на одном конце ВОЛС и восстановление электрических сигналов из оптических – на другом конце. Как показали проведенные нами исследования некоторых типов мультиплексоров [5.14], они не выдерживают даже стандартных импульсных перенапряжений в соответствии с требованиями по электромагнитной совместимости (ЭМС). При повреждении внутренних электронных компонентов мультиплексоров под воздействием ПЭДВ состояние их выходных цепей окажется непредсказуемым. Если такой поврежденный мультиплексор будет не способен передать дистанционную команду на изменение положения выключателя, никакой катастрофы не произойдет, ну а если его выходные цепи окажутся в активированном состоянии, то неприятностей не избежать. То же самое относится и ко всем другим компонентам предлагаемой системы ЗДУВ (модему, контроллеру).

Кроме того, поскольку прокладка выделенных ВОЛС и установка аппаратуры сопряжения достаточно дороги, то уже сегодня существует тенденция отказа от использования выделенных ВОЛС и использования существующих компьютерных сетей на основе дешевых кабелей с витой парой. Более того, с целью еще большего удешевления систем управления, релейной защиты и автоматики, всерьез рассматривается возможность перехода на беспроводные технологии WiFi. Во всяком случае, многие мировые лидеры в производстве МУРЗ, уже сегодня выпускают их со встроенными модемами WiFi.

Собственно говоря, идея перевода всего энергетического оборудования на связи по стандартным компьютерным сетям, включая беспроводные – это центральная идея концепции «Умных сетей» (Smart Grid). В этой связи возрастает актуальность разработки спе-

циальных аппаратных средств защиты и систем релейной защиты, и дистанционного управления коммутационными аппаратами от преднамеренных дистанционных деструктивных воздействий, включающих электромагнитные воздействия и кибератаки, не связанных с компьютерными сетями и обладающих повышенной устойчивостью к ПЭДВ.

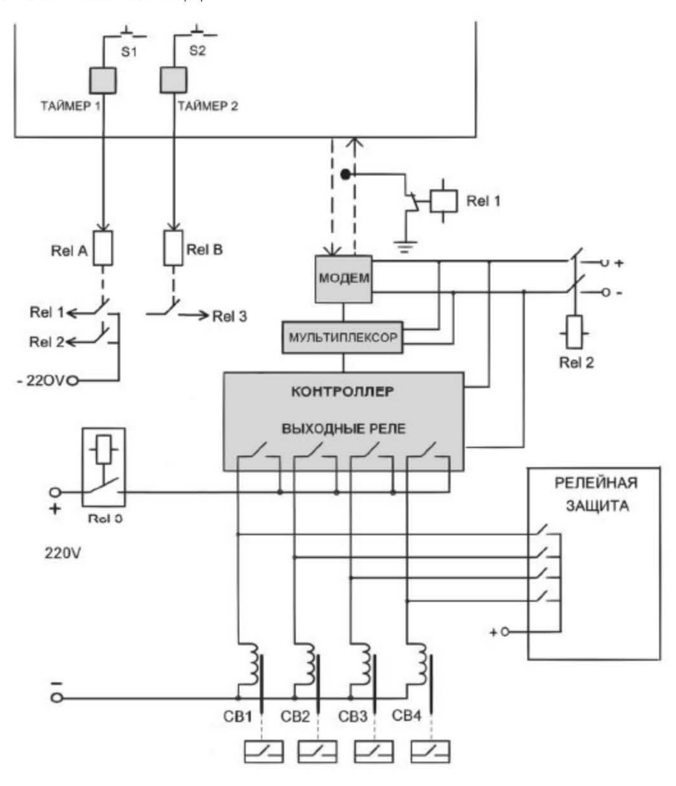


Рис. 5.21. Предлагаемая структура защищенной системы дистанционного управления выключателями (ЗДУВ). Цепи питания показаны условно для упрощения схемы

Именно поэтому в качестве элементов такой защиты нами выбраны электромеханические реле, управляемые оперативным напряжением по контрольным кабелям. С целью защиты этого дополнительного канала связи от злонамеренного внешнего подключения и несанкционированной активации электромеханических реле, используются токоведущие жилы, принадлежащие разным контрольным кабелям, а вместо одного реле используются два реле RelA и RelB рис. 5.21. Естественно, катушки этих реле и токоведущие жилы кабелей, по которым осуществляется их питание должны быть защищены (например, с помощью варисторов) от импульсных перенапряжений, которые могут быть наведены в этих жилах под воздействием мощного электромагнитного импульса ПЭДВ. Кроме того, желательно осуществлять питание этих реле переменным током промышленной частоты с конденсатором, включенным в разрыв цепи питания, а на стороне подстанции использовать разделительный трансформатор. Эти меры позволят предотвратить срабатывание реле RelA и RelB от токов сверхнизкой частоты, наводимых в подземных кабелях под воздействием компонента Е3 электромагнитного импульса.

В тех случаях, когда использование контрольного кабеля для управления реле RelA и RelB не представляется возможным ни при каких условиях из-за значительной удаленности диспетчерского пункта от подстанции, возможно применение ВОЛС в качестве разрешающего канала связи. При этом следует иметь ввиду снижение защищенности системы к ПЭДВ. Для предотвращения самопроизвольной выдачи команд на изменение положения выключателей вследствие повреждения электронных устройств системы, они должны быть снабжены самодиагностикой. Канал ВОЛС – постоянным мониторингом собственной исправности, а также положения реле RelA и RelB, а контроллер – внутренней системой самодиагностики, автоматически запускаемой сразу же при активации реле Rel1 Rel2 и включающей в себя опрос состояния выходных реле (они должны быть выключены) и исправность канала связи. При обнаружении неисправности система самодиагностики должна блокировать дальнейшую работу контроллера. Кроме того, для защиты системы от ПЭДВ должны быть использованы различные методы пассивной защиты, описанные в Гл. 4.

Только при поступлении на диспетчерский пункт информации об исправности всех элементов системы может быть разрешено использование ее для дистанционного управления выключателями.

В предлагаемом устройстве любая команда на изменение положения выключателей, передаваемая по сетевому каналу любого типа, должно сопровождаться кратковременным дистанционным включением двух реле RelA и RelB по контрольному (возможно, оптическому) кабелю. Контакты этих реле включают местные электромеханические промежуточные реле: Rel1 (деблокирует сетевой канал связи), Rel2 (подает питание на электронные устройства системы) и Rel3 (включает цепь питания катушек выключателей). Все эти местные реле могут быть разными по своим характеристикам. Например, Rel1 – высокочастотное реле, Rel3 – реле с мощными контактами, предназначенными для коммутации индуктивной нагрузки на постоянном токе. Наличие двух управляющих реле RelA и RelB с отдельными каналами управления повышает защищенность системы от несанкционированного доступа.

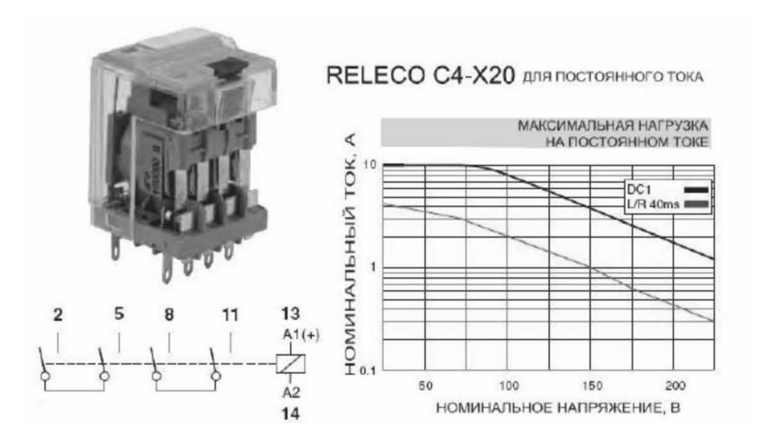


Рис. 5.22. Реле типа C4-X20 фирмы RELECO (с частично удаленным чехлом) с двумя контактами с двойным разрывом и его коммутационная способность на постоянном токе

Первым включается RelA, а после передачи на контроллер необходимой информации об изменении положения того или иного

выключателея и замыкании контактов соответствующего выходного реле контроллера, включается реле RelB и своим контактом включает реле Rel3. Время включенного состояния реле RelA и RelB автоматически ограничивается таймерами с тем, чтобы предотвратить постоянное включение этих реле при ошибке персонала. Реально это короткий промежуток времени, в течение которого осуществить эффективную кибератаку практически невозможно. А блокирование канала связи и отключение питания контроллера вне этого короткого промежутка времени исключает опасность предварительной активации выходных реле контроллера в результате кибератаки с последующим несанкционированным изменением положения выключателей в момент включении электромагнитного реле RelB.

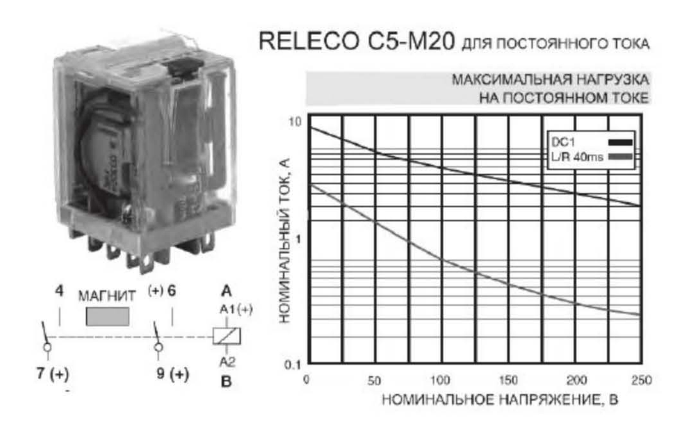


Рис. 5.23. Реле типа C5-M20 фирмы RELECO с двумя замыкающими контактами и дугогасящим магнитом и коммутационная способность его контактов для индуктивной нагрузки

Рис. 5.24. Реле типа RMEA-FT-1 с одним замыкающим контактом с тройным разрывом, способным коммутировать постоянный ток до 3А в индуктивной нагрузке при напряжении 220В (производитель: RELEQUICK S. A.)

Эти же меры резко снижают и вероятность повреждения чувствительной электронной аппаратуры (модем, мультиплексор, контроллер) от повреждения при воздействии ПЭДВ.

После зарегистрированной кибератаки или электромагнитного импульса дистанционное управление выключателями должно быть запрещено до специальной проверки, поскольку состояние контроллера после таких воздействий на него не известно.

Выходные реле контроллера могут быть маломощными стандартными, которыми комплектуются обычные контроллеры. А вот реле Rel3 должно иметь контакты, способные включать достаточно мощную нагрузку индуктивного характера (катушки управления выключателями) на постоянном токе и при напряжении 220 В.

Анализ спецификаций распространенных типов электромагнитных реле показывает, что большинство из них не предназначены для коммутации (и даже для включения) индуктивных нагрузок на постоянном токе с напряжением 220В [5.15]. Для этой цели служат реле специальной конструкции: обеспечивающие многократные последовательные разрывы в коммутируемой цепи (рис. 5.22) или содержащие постоянный магнит вблизи контактов, предназначенный для выталкивания электрической дуги из межконтактного зазора (рис. 5.23).

Имеются также и реле с тремя разрывами на контакт, рис. 5.24, позволяющие управлять отключающими катушками высоковольтных выключателей старого типа с большими потребляемыми токами.

В тех случаях, когда использование контрольного кабеля для управления реле RelA и RelB не представляется возможным из-за значительной удаленности диспетчерского пункта от подстанции, возможно применение ВОЛС в качестве разрешающего канала связи. При этом следует иметь ввиду снижение защищенности системы к ПЭДВ. Для предотвращения самопроизвольной выдачи команд на изменение положения выключателей вследствие повреждения электронных устройств системы, они должны быть снабжены самодиагностикой. Канал ВОЛС – постоянным мониторингом собственной исправности, а также положения реле RelA и RelB, а контроллер – внутренней системой самодиагностики, автоматически запускаемой сразу же при активации реле Rel1 Rel2 и включающей в себя опрос состояния выходных реле (они должны быть выключены) и исправ-

ность канала связи. При обнаружении неисправности система самодиагностики должна блокировать дальнейшую работу контроллера. Только при поступлении на диспетчерский пункт информации об исправности всех элементов системы может быть разрешено использование ее для дистанционного управления выключателями.

Как можно видеть, в обоих случаях, то есть и для защиты МУРЗ и для защиты системы ДУВ используются электромеханические реле, однако применение этих реле различно, что связано с различным алгоритмом работы МУРЗ и ДУВ. Если в первом случае выдача команды на выключатели производится автоматически при изменении контролируемого режима работы электрической сети или энергетического оборудования, то во втором случае, выдача команды на выключатели производится вручную диспетчерским персоналом. С этим связаны и различные принципы реализации защиты. Так, в первом случае важно защитить постоянно работающий в автоматическом режиме МУРЗ от несанкционированного изменения его уставок или внутренней логики, вызывающих срабатывание выходных реле и нет возможности перед активацией выходных реле проверить правильность команд. Кроме того, нет никакой возможности подать на МУРЗ какой-то внешний разрешающий сигнал при возникновении аварийного режима в контролируемой сети и этот разрешающий сигнал должен формироваться на месте, по факту возникновения аварийного режима. Тогда как во втором случае, когда защищаемый объект (ДУВ) не работает в автоматическом режиме, задача значительно упрощается и становится возможным использование внешнего разрешающего сигнала. Кроме того, в критических случаях, ДУВ может быть вообще отменено. Эти естественные различия в принципах организации защиты от преднамеренных деструктивных воздействий еще раз подтверждают целесообразность разделения задач релейной защиты и дистанционного управления выключателями.

Литература к Гл. 5

5.1 Гуревич В. И. Вопросы философии в релейной защите. - Мир техники и технологий, 2013, № 1, с. 56 - 58.

5.2 Гуревич В. И. Кибероружие против энергетики. - PRO Электричество, 2011, №1, с. 26 - 29.

5.3 Гуревич В. И. Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. Ч. 1. - Компоненты и технологии, 2010, № 2, с. 60-64.

5.4 The Impact of Implementing Cyber Security Requirements using IEC 61850. - CIGRE Working Group the B5.38, August 2010.

5.5 Гуревич В. И. Интеллектуальные сети: новые перспективы или новые проблемы? - "Электротехнический рынок", 2010, № 6 (ч. 1); 2011, № 1 (ч. 2).

5.6 Гуревич В. И. О некоторых путях решения проблемы электромагнитной совместимости релейной защиты в электроэнергетике. - Промышленная энергетика, 1996, № 3, с. 25 – 27.

5.7 Гуревич В. И. Электромеханические и микропроцессорные реле защиты. Возможен ли симбиоз? – Релейная защита и автоматизация, 2013, № 2, с. 75-77.

5.8 Гуревич В. И. Устройство защиты релейной защиты. – Control Engineering Россия, 2013, № 3, с. 47- 51.

5.9 Gurevich V. Protection Devices and Systems for High-Voltage Applications. – Marcel Dekker, New York, 2003, 292 p.

5.10 Gurevich V. Electronic Devices on Discrete Components for Industrial and Power Engineering. – CRC Press (Taylor & Francis Group), Boca Raton – London – New York, 2008, 419 p.

5.11 Гуревич В. И. Герконовые реле с регулируемым порогом срабатывания. – Компоненты и технологии, 2013, № 11, с. 30-33.

5.12 Гуревич В. И. Технический прогресс в релейной защите. Опасные тенденции развития РЗА. - "Новости электротехники", 2011, № 5, с. 38 - 40.

5.13 Гуревич В. И. Про многофункциональную релейную защиту. - "PRO Электричество", 2012, № 42-43, с. 45 - 48.

5.14 Гуревич В. И. Актуальные проблемы релейной защиты: альтернативный взгляд. - "Вести в электроэнергетике", 2010, № 3, с. 30 - 43.

5.15 Гуревич В. И. Особенности реле, предназначенных для включения отключающих катушек высоковольтных выключателей - “Электричество”, 2008, № 11, с. 22 - 29.

6. ИСПЫТАНИЕ УСТОЙЧИВОСТИ МУРЗ К ВОЗДЕЙСТВИЮ ПЭДВ

6. 1. Анализ источников ПЭДВ

Требования по устойчивости реле защиты (включая МУРЗ) к электромагнитным воздействиям изложены в стандартах Международной электротехнической комиссии (МЭК) серии 60255. Общие требования по электромагнитной совместимости (ЭМС) к электронной аппаратуре – в стандартах МЭК серии 61000. Стандарты, идентичные серии МЭК 61000, используются и в России. Однако, все эти требования относятся к так называемым «непреднамеренным электромагнитным воздействиям», то есть к воздействиям (помехам) естественного происхождения. Электромагнитные же воздействия искусственного происхождения, специально, предназначенные для поражения электронной аппаратуры (ПЭДВ) оказывают на аппаратуру значительно более сильные воздействия, чем предусмотренные обычными стандартами по ЭМС и поэтому обычные стандарты по ЭМС не могут быть использованы в данном случае.

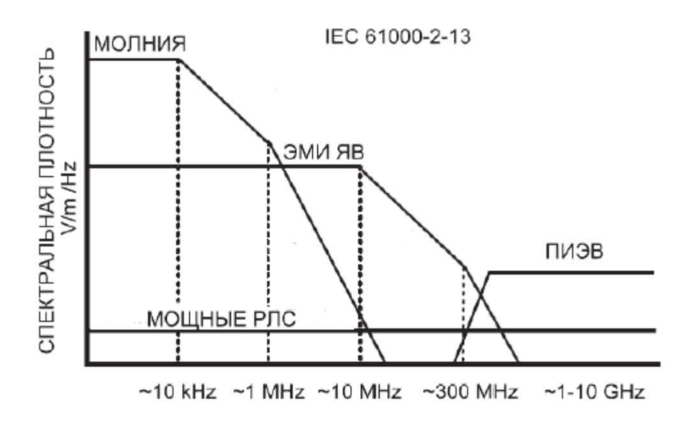


Рис. 6.1. Спектральная плотность излучения различных источников ПЭДВ в соответствии со стандартом IEC 61000-2-13

Для выработки конкретных рекомендаций и технических требований к испытаниям МУРЗ на устойчивость к ПЭДВ необходимо решить несколько задач:

1. Классифицировать типы ПЭДВ и обобщить их технические параметры.
2. Оценить параметры ПЭДВ, воздействующие на МУРЗ в реальных условиях эксплуатации.
3. На основе анализа существующих стандартов в области ПЭДВ сформулировать технические требования к оборудованию, необходимому для симуляции ПЭДВ и испытаниям МУРЗ на устойчивость к воздействию ПЭДВ.
4. Провести анализ рынка оборудования, предназначенного для испытания МУРЗ.

Как можно видеть из рис. 6.1, молния имеет намного большую спектральную плотность электромагнитного излучения, чем даже такой мощный источник излучения, как электромагнитный импульс ядерного взрыва, однако при этом следует иметь в виду, что вся энергия молнии сконцентрирована в так называемом ступенчатом лидере и имеет точечную зону поражения, в то время как ЭМИ ЯВ охватывает обширную поверхность земного шара, рис. 6.2.

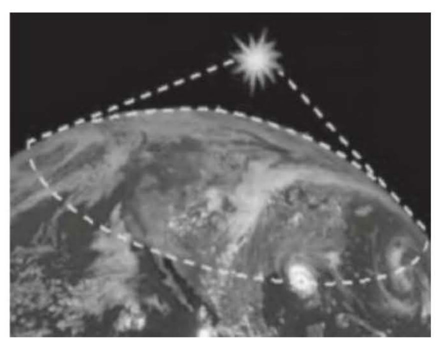


Рис. 6.2. Зона поражения молнии и ЭМИ ЯВ

Каждый из этих классов ПЭДВ делится, в свою очередь, на отдельные виды воздействий. ЭМИ ЯВ включает в себя три различных вида воздействия, в соответствии с тремя составляющими электромагнитного импульса: E1 (early-time), E2 (intermediate-time), E3 (late-time), описанными в Гл. 2.

Поскольку речь идет об испытаниях электронной аппаратуры, то в дальнейшем нас будет интересовать лишь компонент E1, как самый мощный и самый опасный для электронной аппаратуры.

Преднамеренно излучаемые электромагнитные помехи - ПИЭМ (см. Гл. 2) в свою очередь делятся на два вида:

1. Направленное узкополостное или ультраширокополостное электромагнитное излучение (High Power Microwave). Такое излучение может исходить от:

- работающих в непрерывном режиме на фиксированной частоте генераторов;
- генераторов, излучающих пачки высокочастотных импульсов, следующих с частотой от сотен герц до десятков килогерц (рис. 6.3);
- генераторов, излучающих в ультрашироком диапазоне частот от десятков мегагерц до сотен ГГц;
- генераторов, излучающих затухающие по амплитуде высокочастотные сигналы (рис. 6.3);
- импульсных генераторов с излучаемой пиковой мощностью от десятков мегаватт до единиц гигаватт. Эти генераторы генерируют очень короткие импульсы в наносекундном (единицы-десятки наносекунд) и субнаносекундном диапазоне (длительность импульсов десятки-сотни пикосекунд), следующих с частотой 0.1 – 10 кГц и более.

2. Импульсное электромагнитное излучение взрывных источников радиочастотного электромагнитного излучения (РЧЭМИ), большинство из которых основано на использовании ударно-волнового излучателя (УВИ), генерирующего мощный (1 ГВт и более) короткий импульс длительностью менее 1 нс с частотой полученного излучения — от сотен мегагерц до сотен гигагерц в одном импульсе.

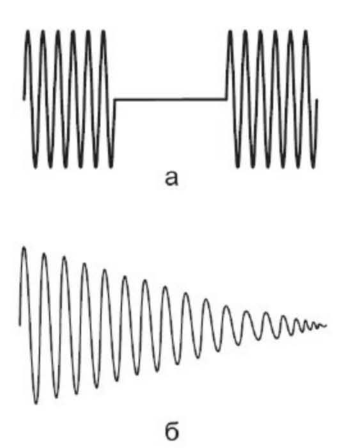


Рис. 6.3. Некоторые типы сигналов источников ПИЭМ, а – пачки высокочастотных импульсов одинаковой амплитуды; б – затухающие по амплитуде высокочастотные импульсы, повторяющиеся с частотой в несколько килогерц

В отличие от приведенной выше классификации, стандарт NATO AECTP 250 Ed 2.0: 2011 Leaflet 257 – High Power Microwave делит ПИЭМ на четыре типа по другому принципу:

а) Мобильный источник РЧЭМИ, направленный в сторону поражаемой цели и расположенный вне охраняемой территории цели, но способный приблизится к ней на достаточно близкое расстояние для эффективного поражения.

б) Портативный источник РЧЭМИ, который может быть доставлен непосредственно в защищаемую зону под одеждой человека или в виде портфеля и установлен в непосредственной близости от поражаемого объекта. Маломощный источник такого типа может быть намного опаснее, чем мощный удаленный источник РЧЭМИ, поскольку его излучение ничем не ослабляется.

в) Контактный источник РЧЭМИ, инжектирующий энергию непосредственно в электрические провода и кабели, соединенные с поражаемой электронной аппаратурой, например, в кабели связи.

Такой источник может быть расположен как внутри, так и вне защищаемой зоны.

г) Источник РЧЭМИ взрывного типа, выполненный в виде электромагнитной бомбы или снаряда, излучающий короткий электромагнитный импульс, проникающий в поражаемую аппаратуру через стены, окна, а также через провода и кабели, выходящие за пределы здания.

Для перечисленных выше источников РЧЭМИ стандарт НАТО указывает максимальную излучаемую антенной мощность 1ГВт/м^2, ограничиваемую электрической прочностью воздуха, равной 1 МВ/м. Следует отметить, что во многих других литературных источниках указывается иное значение для электрической прочности воздуха в нормальных климатических условиях: 2 – 3 МВ/м. Кроме того, даже в неоднородных электрических полях разрядное импульсное напряжение воздуха дополнительно повышается и превышает значение, нормируемое для переменного напряжения 50 Гц. Отношение амплитуды импульсного пробивного напряжения к напряжению при частоте 50 Гц называется коэффициентом импульса k_i. Для неоднородных электрических полей $k_i = 1.1 – 1.3$. Следует, однако, учитывать, что при пониженном давлении воздуха (в высокогорных районах) или при наличии в воздухе пыли и паров влаги (тумане) электрическая прочность воздуха может значительно снизиться. Снижение электрической прочности воздуха наблюдается также в процессе ионизации воздуха под действием высокочастотного разряда. Тем не менее, в 2008 г. в Институте сильноточной электроники Сибирского отделения Российской Академии Наук (ИСЭ СО РАН) недавно был построен сверхширокополостный генератор импульсов, рис. 6.4 с выходной пиковой мощностью 3.4 ГВт, что намного превышает предельный уровень мощности излучения, указанный в стандарте НАТО. Этот генератор работает на напряжениях -205 кВ и +157 кВ и генерирует импульсы длительностью около 1 нс при частоте следования импульсов 100 Гц. А в лаборатории ВВС США, расположенной на авиабазе Киртланд (Albuquerque, New Mexico) еще в 1989 г. был разработан РЧЭМИ с излучаемой мощностью 7.5 ГВт на основе так называемого «виркатора» (генератора с виртуальным катодом), работающего при напряжении 4 МВ и токе 80 кА [6.1]. С тех пор конструкцию виркатора удалось

существенно усовершенствовать, повысить мощность до 40 ГВт, улучшить КПД. Это, в свою очередь, позволило смонтировать мощный направленный генератор РЧЭМИ на базе виркатора в головной части крылатой ракеты, которая по трассе своего полета способна сжигать всю наземную микроэлектронику и компьютерную технику, не имеющую специальной защиты.

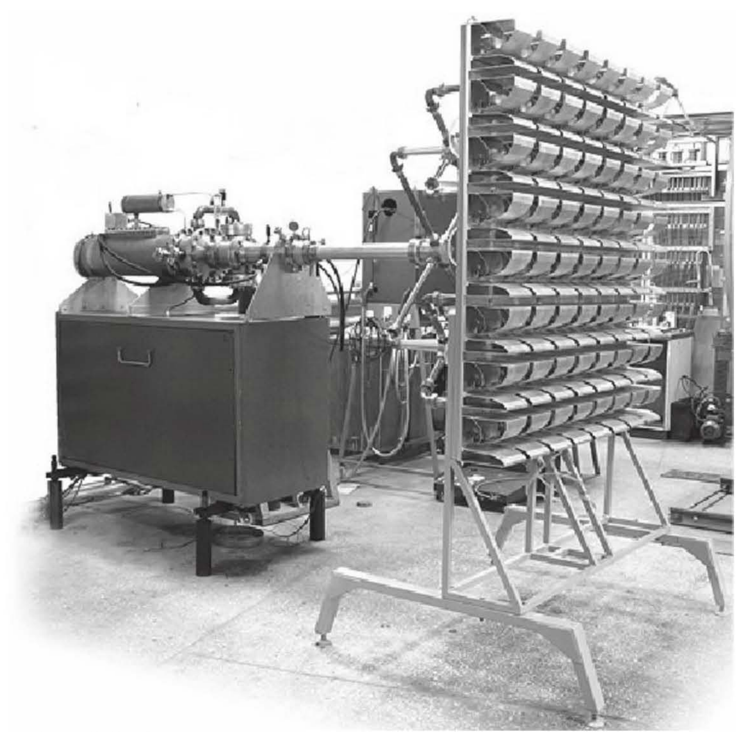


Рис. 6.4. Генератор ультраширокополостных импульсов с пиковой излучаемой мощностью 3.4 ГВт, разработанный ИСЭ СО РАН

Секретный проект, начатый в 2008 году [6.2] завершился полным успехом, о чем сообщили многие средства массовой информации, охарактеризовав этот успех, как наступление новой эры в будущих войнах.

6.2 Параметры испытаний на устойчивость к ЭМИ ЯВ

В соответствии со стандартом 61000-4-25, испытания на устойчивость электронной аппаратуры к ЭМИ ЯВ должны содержать две составные части: испытание на устойчивость к электромагнитным излучениям (ЭМИЗ) и к контактным импульсным воздействиям (КИВ). В свою очередь контактные импульсные воздействия подразделяются на два вида: импульсные напряжения, прикладываемые к входам аппаратуры и импульсные токи, наводимые в протяженных проводах и кабелях.

Определение конкретных норм испытаний начинается с выбора одной из 6 концепции испытаний. Стандарты 61000-2-11 и 61000-5-3 определяют эти концепции. Для МУРЗ, расположенных в капитальных железобетонных или кирпичных зданиях, снабженных защитой от молний, без специальных защитных фильтров может быть выбрана концепция номер 2b. Этой концепцией предусматривается ослабление конструкцией здания уровня ЭМИЗ на 20 дБ в полосе частот 100 кГц – 30 МГц. Для выбранной концепции и компонента E1 напряженность электрического поля излучения, воздействующего на испытуемый объект устанавливается 5 кВ/м (уровень R4), напряженность магнитного поля 13.3 А/м.

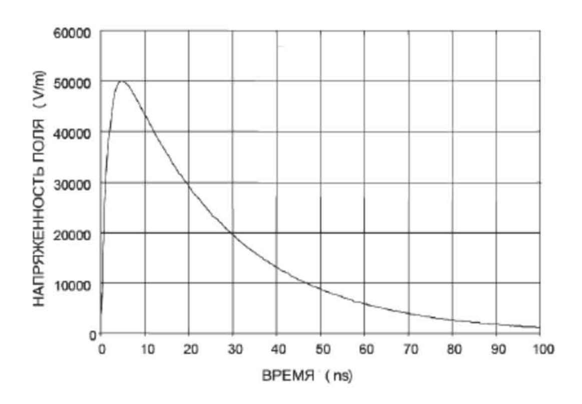


Рис. 6.5. Форма компонента ЭМИЗ в соответствии со стандартами IEC 61000-2-9, IEC 61000-2-10, IEC 61000-2-11 и MIL-STD-461F

Для сравнения: для деревянных зданий, не ослабляющих ЭМИЗ, напряженность электрического поля составляет 50 кВ/м (уровень R7).

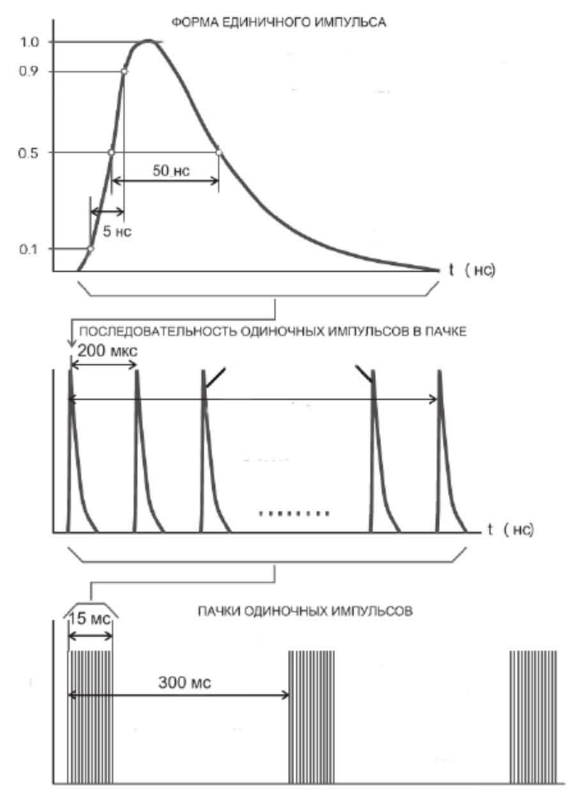


Рис. 6.6. Electrical Fast Transient (EFT) – быстрый импульс (IEC 61000-4-4)

Для той же концепции и компонента Е2 напряженность электрического поля устанавливается 10 В/м и магнитного поля 0.08 А/м. Параметры импульса ЭМИЗ описаны в стандартах 61000-2-9, 61000-2-10, 61000-2-11, MIL-STD-461F: время нарастания импульса

(передний фронт) 2.5 нс, ширина импульса 25 нс, форма импульса соответствует приведенному на рис. 6.5.

В таблице 1 этого стандарта амплитуда испытательного нпряжения для HEMP (обозначен как “special”) отмечена значком «X» и соответствует для него уровням E8 или E9.

На следующем этапе выбирается уровень испытательного воздействия для КИВ в соответствии со стандартом 61000-4-25. Для выбранной концепции номер 2b и наличии подключенных к рассматриваемому объекту незаглубленных в грунт проводов выбирается уровень испытательного воздействия E8 (для обеспечения нормальной 50% вероятности устойчивости объекта) или E9 (для 99% вероятности). Уровень E8 предполагает устойчивость испытуемого объекта к импульсному напряжению 8 кВ, а уровень E9 – 16 кВ. Вероятность 50% считается в стандарте нормальной и может применяться для гражданской аппаратуры.

Под испытательным импульсом напряжения КИВ подразумевается так называемый Electrical Fast Transient (EFT) – быстрый импульс, параметры которого (кроме амплитуды испытательного напряжения) и методика испытаний описаны в стандарте IEC 61000-4-4, рис. 6.6.

6.3 Параметры испытаний на устойчивость к ПИЭМ

Как отмечалось выше, стандарт МЭК (IEC 61000-4-36) с параметрами испытаний на устойчивость к ПИЭМ еще не опубликован, однако, имеются другие стандарты и результаты исследований, характеризующие параметры ПИЭМ [6.3 – 6.15]. В настоящее время существует несколько принципиально различных методов генерации мощных РЧЭМИ, которые могут быть использованы для дистанционного поражения электронных и компьютерных систем, что обуславливает очень широкий диапазон параметров излучения:

- напряженность электрического поля в диапазоне от 1 до 100 кВ/м;
- длительность фронта импульса - от 100 до 500 пс;
- длительность импульса - от сотен пикосекунд до единиц наносекунд;
- частота повторения импульсов - от 0,1 до 1000 Гц.

Совершенно очевидно, что при наличии такого широкого разброса параметров разработанных источников, очень сложно установить какие-то четкие требования к испытаниям электронной аппаратуры на устойчивость к этим излучениям. Тем не менее, на основе исследований, выполненных ведущим специалистом в этой области Вильямом Радаски (William Radasky), можно говорить о широкополостном импульсном излучении с длительностью фронта импульса 100 пс, шириной импульса 1 нс, частотой следования импульсов 1 МГц и напряженностью поля 10 кВ/м [6.7]. По имеющимся у автора сведениям, эти же параметры должны войти и в стандарт IEC 61000-4-36.

6.4 Испытательное оборудование для тестирования на устойчивость к ПЭДВ

Разработкой источников мощных импульсов и РЧЭМИ занимаются множество организаций во многих странах мира:

1. Институт сильноточной электроники СО РАН (г.Томск);
2. Институт электрофизики УрО РАН (г.Екатеринбург);
3. Институт радиотехники и электроники РАН (г.Москва);
4. Институт прикладной физики РАН (г. Нижний Новгород)
5. Всероссийский научно-исследовательский институт экспериментальной физики, г.Саров
6. Московский радиотехнический институт РАН (г.Москва);
7. Институт высоких температур РАН (г.Москва);
8. СКБ НП УрО РАН (г. Екатеринбург);
9. СКБ НП СО РАН (г.Томск);
10. Московский государственный университет;
11. Уральский политехнический институт, (г.Екатеринбург);
12. ПО Томсктрансгаз (г.Томск);
13. Научно-исследовательский институт полупроводников, (г.Томск);
14. НПО "ЗЕНИТ" (г.Зеленоград);
15. НПО "БУРЕВЕСТНИК" (г. Санкт-Петербург)
16. Высоковольтный научно-исследовательский центр ВЭИ (ВНИЦ ВЭИ), Москва
17. Техасский технический университет, (г.Лаббок, США);
18. Advanced Physics, Inc., (г. Эрвайн, США);

19. Исследовательский центр GEC-Marconi, (г.Челмсфорд, Великобритания);

20. Исследовательский центр ядерной физики SOREQ (г. Явне, Израиль)

21. Rafael Advanced Defense Systems (Хайфа, Израиль)

22. Исследовательский центр DSTO (г.Солсбери, Австралия);

23. Университет Стразклайд (г. Глазго, Великобритания);

24. Институт физики, (г.Тарту, Эстония)

20. Исследовательский центр FOA (г. Линчопинг, Швеция)

25. Северо-западный Институт ядерных технологий (г. Сиань, Китай)

26. Исследовательская лаборатория RMA (г.Брюссель, Бельгия) Ю

27. Исследовательский центр DSO (Сингапур)

28. Исследовательский центр Diehl Shtiftung (г. Ретенбах на Пегнице, Германия)

29. Aviation University of Air-Force Changchun, Китай

30. Electrostatic and Electromagnetic Protection Research Institute, Китай

31. University of Electronic Science and Technology, Китай

32. Beijing Key Laboratory of High Voltage &EMC, Китай

33. North China Electric Power University, Китай

34. Key Laboratory of Power System Protection and Dynamic Security Monitoring and Control, Китай

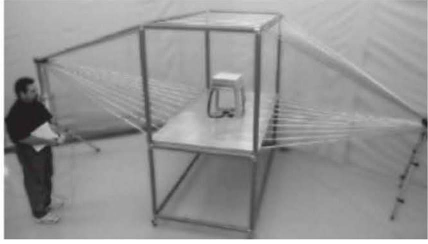
35. Nanjing Engineering Institute No.1, Китай

36. Jilin University, Китай

Однако, продукция большинства этих организаций предназначена для выполнения собственных исследований и не предназначена для продажи на рынке в качестве симуляторов ЭМИЗ или ПИЭМ для целей тестирования электронной аппаратуры. Большинство крупных производителей военной техники имеют собственные испытательные стенды для испытаний образцов производимой ими продукции, рис. 6.7, также не предназначенные для продажи. Подобными стендами, обладают производители военной техники в Канаде, Китае, Франции, Германии, Индии, Израиле, Италии, Голландии, России, Швеции, Украине, Великобритании и США. Некоторые из них подробно описаны в стандарте IEC/TR 61000-4-32.

Рис. 6.7. Испытательный стенд для симуляции воздействиям ЭМИ ЯВ на военную технику

Рис. 6.8. Стационарный имитатор ЭМИ ЯВ «Аллюр» Высоковольтного научно-исследовательского центра ФГУП ВЭИ (г. Истра, Московской обл.). Габариты имитатора: 100 х 35 х 13,5 м; рабочий объем: 10 х 10 х 10 м; форма импульса: 2,5/25 нс; максимальная напряженность импульса электрического поля: 70 кВ/м



а б

Рис. 6.9. Компактные стенды для испытания электронной аппаратуры на устойчивость к ЭМИЗ. а- Montena Technology, б - Applied Physical Electronics

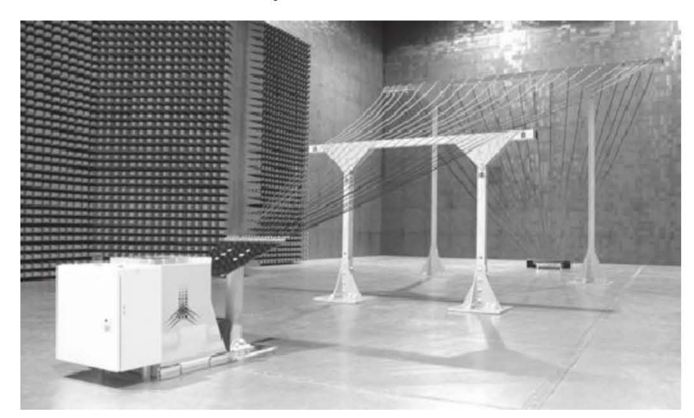


Рис. 6.10. Испытательный стенд, производимый на продажу компанией Montena Technology (США) для лабораторных испытаний более крупных объектов, например таких, как шкафы релейной защиты на устойчивость к ЭМИ ЯВ. Слева виден генератор импульсов, справа – антенная система

Во многих странах имеются также специализированные испытательные лаборатории, принимающие заказы на проведение испытаний такого рода от посторонних организаций. В России это, например, испытательный комплекс «Аллюр» Высоковольтного научно-исследовательского центра ВЭИ в г. Истре Московской обл., рис. 6.8. Однако компаний, производящих на продажу тесто-

вое оборудования для проведения испытаний на устойчивость к ПЭДВ в соответствии со стандартами, мире очень немногоКрупные установки, предназначенные для симуляции ЭМИЗ, выпускаются компаниями Dayton T. Brown (США), Aero-Rad Technology Co., Ltd (Китай) и некоторыми другими. Небольшие испытательные установки, пригодные для лабораторных испытаний электронной аппаратуры типа МУРЗ на устойчивость к ЭМИЗ выпускаются лишь двумя компаниями: швейцарской Montena Technology и американской Applied Physical Electronics, рис. 6.9.

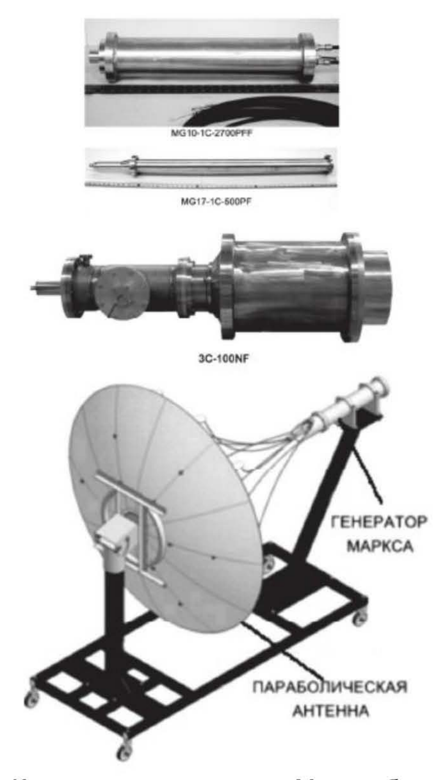


Рис. 6.11. Компактные генераторы Маркса большой мощности MG10-1C-2700PFF (300 кВ, 1 ГВт); MG17-1C-500PF (510 кВ, 400 МВт); MG30-3C-100NF (600 кВ, 6 ГВт) и источник РЧЭМИ на основе этих генераторов с направленной параболической антенной

Компания Montena Technology выпускает множество видов испытательной аппаратуры, в том числе и достаточно крупных стендов (высота 1.8 м, полная длина 7 м), пригодных для испытаний целых шкафов с электронной аппаратурой, например, шкафов релейной защиты, рис. 6.10.

Что касается испытательного оборудования для тестирования электронной аппаратуры на устойчивость к ПИЭМ, то в качестве такого оборудования могут быть использованы компактные генераторы Маркса различной мощности, снабженные направленной антенной, предлагаемые в широком ассортименте компанией Applied Physical Electronics, рис. 6.11.

Табл. 6.1. Максимальная амплитуда импульса 5/50 нс выходного напряжения генераторов EFT (IEC 61000-4-4), имеющихся на рынке

Тип EFT генератора	Производитель	Максимальная амплитуда выходного импульсного напряжения, кВ
PEFT 8010	Haefely EMC Technology	7.3
NSG 2025*	TESEQ	8
J0101031/3*	Kentech Instruments Ltd.	8
KeyTek ECAT E421*	Thermo Electron Corp.	8
FNS-AX3-A16B	NoiseKen Laboratory Co.	4.8
EFT 500N8	EMTEST	7
TRA3000	EMC Partner	5
EFT 6501	Schaffner	4.4
EFT-4060B	Shanghai Yi PaiElectronmagneticTechn.	6.6
EFT500	Suzhou 3Ctest Electronic Co.	5
AXOS8	Hipotronics	5

*выпуск прекращен

Гораздо сложнее обстоит дело с испытательным оборудованием для тестирования на устойчивость электронной аппаратуры к КИВ

(Electrical Fast Transient - EFT), рис. 6.12. Ранее генераторы EFT с требуемым уровнем выходного напряжения 8 кВ выпускались компаниями TESEQ, Kentech Instruments Ltd. и Thermo Electron Corp. (табл. 6.1) на основе вакуумного управляемого разрядника, формировавшего тестовые импульсы. С появлением мощных полупроводниковых коммутирующих элементов – IGBT-транзисторов, выпуск генераторов на вакуумных разрядниках был прекращен всеми тремя компаниями, поскольку импульсы, формируемые транзисторами, оказались намного более стабильными и «правильными», чем импульсы, формируемые вакуумным разрядником. К сожалению, одновременно с повышением стабильности генерируемых импульсов, пришлось снизить их амплитуду.

Выполненный нами анализ показал, что на сегодняшний ни один из выпускаемых на продажу генераторов EFT не удовлетворяет полностью требованиям стандартов по амплитуде импульса (8 кВ). Наиболее близким к требуемому значением амплитуды импульса обладает генератор типа PEFT 8010, производимый шведской компанией Haefely EMC Technology, рис.6.12.

Рис. 6.12. Генератор EFT типа PEFT 8010 с с максимальной амплитудой импульсов 7.3 кВ, выпускаемый компанией Haefely EMC Technology (Швеция), а – вид на переднюю панель, в – вид задней панели

Таким образом, для испытаний МУРЗ на устойчивость к ПЭДВ необходимы три типа воздействий, проводимых в дополнение к

полному комплексу испытаний на электромагнитную совместимость [6.17]:

1) импульсное электромагнитное излучение с длительностью фронта импульса 2 нс, шириной импульса 25 нс и с напряженностью поля 5 – 50 кВ/м;
2) импульсное электромагнитное излучение с длительностью фронта импульса 100 пс, шириной импульса 1 нс, частотой следования импульсов 1 МГц и напряженностью поля 10 кВ/м;
3) быстрый импульс 5/50 нс (EFT) с амплитудой импульса 8 кВ, подаваемый контактным способом на входы МУРЗ;

Компактная испытательная аппаратура с параметрами, достаточно близкими к требуемым, имеется на рынке в свободной продаже. Это делает вполне возможным и доступным организацию специализированной лаборатории по проверке устойчивости современных устройств релейной защиты и других видов так называемой «критической» электронной аппаратуры промышленного назначения на устойчивость к преднамеренным электромагнитным деструктивным воздействиям. Стоимость комплекта оборудования для такой лаборатории составляет около 500 тыс. долларов США.

6.5 Использование критерия качества функционирования при испытаниях электронной аппаратуры на электромагнитную совместимость (ЭМС)

Реакция испытуемого объекта (ИО) на электромагнитные воздействия (ЭВ) может быть различной. Например, ИО может полностью выйти из строя из-за электрического пробоя электронных компонентов, а может лишь временно потерять работоспособность лишь на время воздействия импульса или электромагнитного поля. Еще один вариант – кратковременный сбой в работе программного обеспечения под действием приложенного к ИО импульсного напряжения, требующий (или не требующий) последующей перезагрузки внутренней программы ИО оператором. Вариантов видов реакции ИО на ЭВ может быть множество. Допустимый для данного типа ИО и для данного типа испытаний вид реакции ИО на элек-

тромагнитные воздействия называется «критерием качества функционирования» (ККФ). Критерий качества функционирования является важнейшим показателем при испытаниях на ЭМС так как от его правильного выбора зависит вывод о том, прошло ли данное устройство какое-то конкретное испытание успешно, или нет. Однако, в стандартах на ЭМС нет, да и не может быть методики правильного выбора этих критериев. Как правило, все ограничивается фразой типа: «*Выбор степеней жесткости, критериев качества функционирования осуществляют лица, разрабатывающие, согласовывающие и утверждающие технические задания или технические условия*» и таблицей из которой можно выбрать тот или иной ККФ из 3 – 4 предлагаемых конкретным стандартом. Это и понятно, поскольку правильный выбор зависит от конкретного типа ИО и конкретных режимов и условий его работы. Более того, для одного и того же типа ИО могут быть выбраны различные ККФ в зависимости от конкретного режима его работы, схемы включения, назначения, по которому он используется, условий эксплуатации и т.д. Поэтому понимание специфических особенностей каждого конкретного ИО является очень важным, поскольку выбор того или иного ККФ обуславливает принятие решения о пригодности или непригодности данного ИО к эксплуатации в конкретных условиях по результатам испытания.

6.6 Особенности использование критерия качества функционирования при испытаниях микропроцессорных устройств релейной защиты на устойчивость к ПЭДВ

Организацией NERC (North American Electric Reliability Council) по запросу специальной комиссии Конгресса США “Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack» составлен список энергетического оборудования, которое должно быть проверено на устойчивость к воздействию электромагнитного импульса высотного ядерного взрыва (ЭМИ ЯВ). В этот список вошли, в частности, микропроцессорные устройства релейной защиты (МУРЗ) и устройства системы SCADA (Supervisory Control and Data Acquisition - общее название программно-аппаратных комплексов различных типов, обеспечивающих сбор данных в режиме реального времени с многочисленных

датчиков, обработку, архивирование, отображение и передачу информации об объектах мониторинга, а также передачу команд оператора на удаленные объекты - основа современной АСУ ТП подстанции). Компанией Metatech были проведены испытания МУРЗ типа SEL-311L (дифференциальная защита линий) и контроллера системы SCADA типа SEL-2032, рис. 6.13, по ускоренной программе и только на устойчивость к составляющей Е1 ЭМИ ЯВ. Результаты этих испытаний представлены в отчете Meta-R-320 [6.16]. Как показано в этом отчете, в качестве ККФ при испытаниях МУРЗ и контроллера SCADA были выбраны оценка исправности функционирования и отсутствие повреждений ***после каждого испытания***, связанного с подачей коротких (5/50 нс) высоковольтных импульсов с амплитудой до 8 кВ на различные входы устройств. Как отмечено в отчете, при подаче импульсов с амплитудой 3.2 кВ на последовательный порт, МУРЗ самопроизвольно выключалось, но потом возвращалось в нормальный режим работы. Некоторые другие порты (например, IRIG - Inter-Range Instrumentation Group time code – порт синхронизации времени) были повреждены уже при напряжении 600 В. В контроллере SCADA был поврежден модуль связи Ethernet при напряжении 1.2 кВ.

Рис. 6.13. МУРЗ типа SEL-311L и контроллер для системы SCADA типа SEL-2032 производства Schweitzer Engineering Laboratories (США) подвергнутые испытаниям на устойчивость к ЭМИ ЯВ

В отчете отмечается, что в качестве одного из дополнительных параметров ККФ, была выбрана запись результатов осциллографирования токов и напряжений приложенных к входам реле. В отчете

сообщается, что в процессе испытаний нарушений в записи обнаружено не было.

6.7 Критика используемого в [6.16]метода испытаний МУРЗ

1. По нашему мнению, использование ККФ, основанных на проверке исправности МУРЗ ***после воздействия*** на него помехи является не правильным и не позволяет прийти к однозначному выводу об устойчивости МУРЗ к этой помехе. Связано это с тем, что МУРЗ обладает некоторыми специфическими особенностями по сравнению с системой SCADA, рассмотренными в [6.17, 6.18]. При всей важности и ответственности системы SCADA, она предназначена, прежде всего, для автоматического сбора, обработки и отображения информации. Несмотря на то, что в состав системы входят так называемые Remote Terminal Units (RTU) – дистанционно управляемые исполнительные устройства, они не могут работать в автоматическом режиме и предназначены лишь для исполнения команд оператора с удаленного диспетчерского пункта. Большинство современных подстанций работают в автоматическом режиме без человека. Ручное управление положением выключателей на таких подстанциях (то есть, фактически, управление конфигурацией электрической сети) осуществляется оператором с диспетчерского центра через систему SCADA, отличающиеся уязвимостью к воздействию ПЭДВ. Поэтому, в случае воздействия ПЭДВ телеуправление подстанцией с диспетчерского пункта с большой степенью вероятности будет потеряно и конфигурация электрической сети будет определяться лишь системой релейной защиты – единственной системой, способной автоматически воздействовать на положение выключателей. При этом, МУРЗ, составляющие основу современной релейной защиты, постоянно обмениваются между собой информацией и командами ***в автоматическом режиме по уязвимым к ПЭДВ каналам связи*** (в отличие от системы SCADA, в которой критические команды управления на выключатели поступают только по инициативе диспетчера). В случае неправильных действий автоматически функционирующей релейной защиты, в работу которой диспетчер уже не может вмешаться, в частности, излишних срабатываний под действием ПЭДВ, электрическая сеть, а за ней и энергосистема в целом, может быть полностью развалена. Это одна

из причин, вследствие которой микропроцессорная релейная защита должна испытываться на воздействие ПЭДВ ***в процессе ее функционирования***, а не проверяться на наличие повреждений после воздействия на нее помехи.

2. Пути проникновения в МУРЗ электромагнитной помехи в виде импульсов, подаваемых на защищенные в большинстве случаев входы и высокочастотной электромагнитной волны, проникающей непосредственно на внутренние высокочув-ствительные электронные компоненты или через незащищенные входы/выходы электронных блоков, а также через многочисленные кабели, подключаемые к МУРЗ и выполняющие роль антенн, абсорбирующих электромагнитную энергию - различны. Тем более, что ПЭДВ не ограничиваются лишь ЭМИ ЯВ, а включают в себя также направленное ультраширокополостное высокочастотное излучение специальных источников мощностью в несколько Гигаватт, предназначенных для дистанционного поражения электронной аппаратуры [6.18]. К сожалению, опасность представляет не только специально предназначенная для поражения электроники аппаратура, но даже излучение обычных мощных радаров. Так, например, в 1999 году был официально зарегистрирован случай катастрофического отказа системы SCADA компании San Diego County Water Authority, обеспечивающей водоснабжение водой города Сан Диего, излучением корабельного радиолокатора, находящегося на расстоянии 25 миль от города. Аналогичный случай произошел в 1980 г. в Голландии на газопроводе, расположенном в полутора километрах от порта Den Helder. Тогда повреждение системы SCADA портовым радаром привело к мощному взрыву газа. Поэтому испытания устойчивости МУРЗ к воздействию ПЭДВ не должно ограничиваться только лишь подачей импульсов высокого напряжения на определенные входы, а должно сопровождаться также облучением ИО электромагнитным излучением с направленной антенны, как это и предусмотрено соответствующими стандартами.

3. Следует учитывать, что в случае возникновения ЭМИ ЯВ его воздействию будет подвергаться не только высокочувствительное электронное оборудование (МУРЗ, аппаратура системы SCADA), но и силовое электрооборудование энергосистем: линейные изоляторы, трансформаторы, генераторы. Причем, воздействовать на это оборудование будет не только составляющая Е1 ЭИМ ЯВ (смоде-

лированная в испытаниях [6.16]), но и две других его составляющих: E2 и E3. Как известно из ранее выполненных исследований [6.16] в Советском Союзе и в США, в результате такого комплексного воздействия всех составляющих ЭМИ ЯВ очень велика вероятность повреждения силового высоковольтного оборудования: пробоя линейных изоляторов, насыщения и сгорания силовых трансформаторов, пробоя изоляции генераторов и т.п. То есть, момент воздействия мощной электромагнитной помехи на МУРЗ совпадает по времени с моментом изменения внутреннего состояния элементов МУРЗ, связанного с появлением на его входах аварийных значений контролируемых токов и напряжений. Как поведет себя МУРЗ в таком режиме? Сможет ли релейная защита, подвергшаяся воздействию ПЭДВ, своевременно отключить входящий в насыщение трансформатор, поврежденный участок воздушной линии, пробитый кабель? Не вызовут ли совместные неправильные действия различных МУРЗ полный развал и коллапс энергосистемы?

Проведенное в [6.16] испытание не дает ответов на эти вопросы. «*Мы произвели системы столь усложненные, что уже не можем предусмотреть все возможные взаимодействия в ней, все возможные отказы. Мы добавляем в эти системы все новые устройства безопасности, но остаемся обманутыми и побежденными скрытыми связями в этих системах*» - писал известный специалист по надежности и уязвимости сложных систем Чарльз Перроу [6.19]. Перроу называет эту проблему "непостижимостью" поскольку даже самый обычный несчастный случай инициирует взаимодействия, которые “не только неожиданны, но и непредсказуемы» для некоторого критического промежутка времени.” В большинстве несчастных случаев никто не ожидал, как одни «алгоритмы взаимодействия» затронут другие, таким образом, никто не мог заранее предполагать то, что случалось. Все это в полной мере относится к современной весьма сложной и разветвленной системе релейной защиты, поведение которой при воздействии ПЭДВ на энергосистему заранее предусмотреть невозможно.

6.8 Анализ результатов второго независимого испытания МУРЗ того же типа

Еще об одном испытании МУРЗ того же самого типа (по странному совпадению) сообщается в рекламной презентации производителя этих устройств - компании Schweitzer Engineering Laboratories [6.20], в которой приведены результаты испытаний образцов МУРЗ типа SEL-311L на испытательных стендах полигона Пикатинни армии США в Нью-Джерси при испытаниях на ЭМИ ЯВ и на электромагнитное излучение, рис. 6.14. В этой рекламной презентации утверждается, что все испытания прошли успешно. Вместе с тем, при более тщательном анализе этого материала выявляются несколько несуразностей. Например, в приведенном на рис. 6.15 рекламном объявлении утверждается, что SEL-311L был испытан при напряженности поля в пределах от 25 до 1000 В/м, в то время как военный стандарт Mil-Std 461 требует всего лишь 50 В/м.

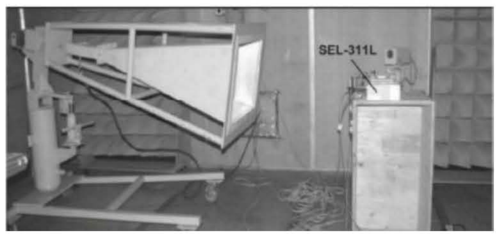


Рис. 6.14. Испытание МУРЗ типа SEL-311L на воздействие ПЭДВ на испытательных стендах полигона Пикатинни армии США в Нью-Джерси [6.20]

SEL-311C Tested at US Army's Picatinny Arsenal in New Jersey

RF from 100 MHz to 4 GHz at power levels from 25 to 1000 volts per meter (Mil-Std 461 ask for 50V/m only)

Рис. 6.15. Текст из рекламного проспекта компании SEL [6]

Довольно странную неосведомленность демонстрируют в этом документе специалисты такой серьезной компании, как SEL, если учесть, что в MIL-STD-461 напряженности полей, соответствующие ПЭДВ рассматриваются не в Вольтах, а в киловольтах и цифра «50» там упоминается не как 50 В/м, а как 50 кВ/м.

Еще более странной выглядит столбчатая диаграмма, представленная на рис. 6.16, из которой видно, что на самом деле напряженность поля в 1000 В/м была использована при испытаниях лишь на частотах 1000 – 1500 МГц, а в остальном частотном диапазоне напряженность поля была чуть ли не вдвое меньше, а зависимость амплитуды от частоты не соответствует MIL-STD-461.

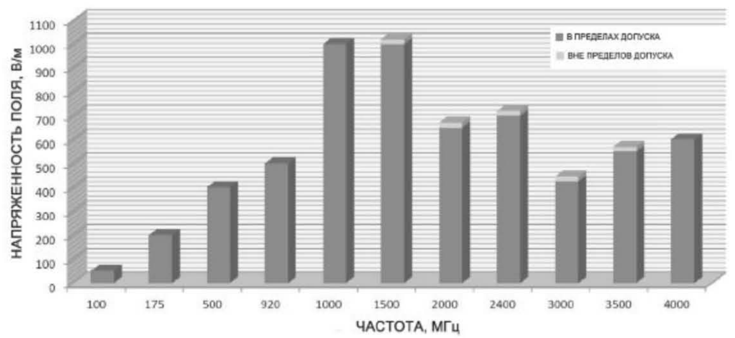


Рис. 6.16. Параметры электромагнитного излучения при испытаниях МУРЗ типа SEL-311L [6.20]

Как можно видеть из представленной диаграммы, уровни напряженности поля на ней ограничиваются началом нестабильности в функционировании реле (желтые области на верхушках столбцов). То есть, фактически, на этой диаграмме представлена область стабильной работы отдельно установленного (то есть, вне

системы релейной защиты) терминала типа SEL. Отсюда следует, что вне области значений, представленных на этой диаграмме, с ее чрезвычайно низкими значениями напряженностей электромагнитного поля, реле не обеспечивает стабильное функционирование. Если сравнить ее с нормами упомянутого стандарта MIL-STD-461, рис. 6.17, то можно заметить, что применявшиеся параметры испытательных воздействий даже близко не приближается к требованиям этого стандарта.

Учитывая такую несуразность в выборе параметров испытаний на устойчивость SEL-311L к ПЭДВ можно ли серьезно относиться к утверждению производителя этих реле об устойчивости его изделий к ПЭДВ?

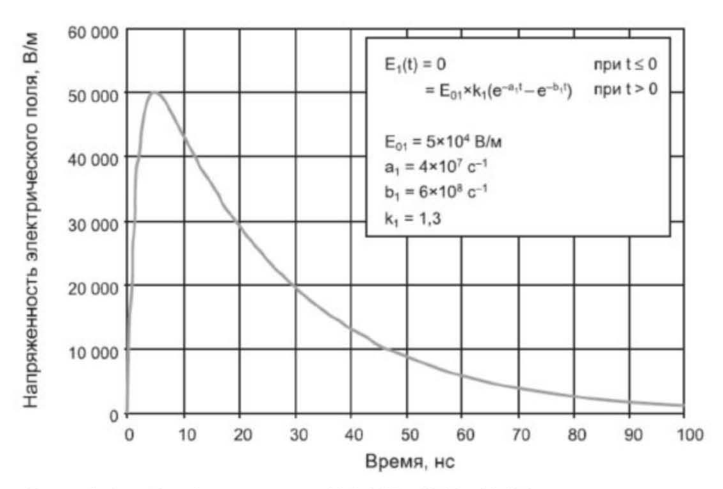


Рис. 6.17. График со стр. 138 MIL-STD-461E для сравнения с диаграммой, приведенной на рис. 6.16 (1 нс соответствует частоте в 1 ГГц)

Еще одна проблема связана с выбором в качестве ИО одиночного терминала МУРЗ. Такие терминалы, как правило, выполняются в металлических корпусах, эффективно ослабляющих электромагнитное излучение, поэтому результаты испытаний на устойчивость к воздействию электромагнитного излучения на такой отдельно взятый терминал вполне ожидаемо могут быть положительными. В

реальных условиях эксплуатации к МУРЗ подключены многочисленные кабели, выполняющие роль антенн, абсорбирующих электромагнитную энергию и доставляющую ее к внутренним элементам МУРЗ; многочисленные терминалы МУРЗ соединены между собой через соответствующую аппаратуру связи, подверженную влиянию ПЭДВ. Поэтому, испытаниям должна подвергаться система релейной защиты, причем, в процессе ее функционирования, а не отдельно взятый терминал.

Примером правильного подхода к испытаниям сложных систем, к которым несомненно относится и релейная защита, может служить испытание системы SCADA, описанное в [6.21], рис. 6.18.

Рис. 6.18. Испытание системы SCADA на устойчивость к ЭМИ ЯВ [6.21]. Вверху видна антенная система симулятора ЭМИ. Элементы системы SCADA расположены в отдельных боксах и соединены между собой стандартной системой связи

Таким образом, получается так, что имея результаты двух независимых испытаний одного и того же типа МУРЗ, проведенных двумя различными исполнителями, невозможно сделать никакого вывода о реальной его устойчивости к ПЭДВ. Кому же нужны такие испытания?

6.9 Выводы и рекомендации по испытаниям МУРЗ

1. Из-за методических ошибок при испытаниях МУРЗ, проведенных ранее независимыми организациями, их нельзя признать удовлетворительными, а результаты значащими. В настоящее время нет достоверных данных о степени устойчивости МУРЗ к ПЭДВ и поэтому такие испытания должны быть проведены повторно.

2. Виды и режимы испытаний МУРЗ должны быть выполнены в полном объеме и соответствовать специальным стандартам.

3. В качестве ККФ должен быть выбран критерий, позволяющий контролировать функционирование МУРЗ в нормальном и аварийном режиме защищаемого объекта в процессе воздействии на него электромагнитной помехи, а не критерий, основанный лишь на проверке исправности терминала после окончания воздействия помехи.

4. Испытанию должен быть подвергнут как отдельный терминал МУРЗ, так и система устройств, включающих в себя несколько МУРЗ, соединенных между собой кабелями длиной не менее нескольких метров через соответствующие устройства связи. При этом облучению электромагнитной энергией должна быть подвергнута вся система, а импульсным испытаниям приложенным напряжением как отдельные терминалы и устройства связи, так и несколько объединенных терминалов и устройств связи одновременно.

5. При проведении испытания должны быть выбраны несколько ступеней по амплитуде испытательных импульсов и напряженности электрического поля: от минимального до максимального значения из приведенных в стандартах диапазонов. Полученные данные должны быть использованы при оценке устойчивости МУРЗ, смонтированных в конкретных шкафах и зданиях, обладающих определенным коэффициентом ослабления электромагнитного поля, а также при выработке требований по дальнейшему ослаблению этого поля, если окажется, что при существующих условиях не обеспечивается требуемая устойчивость МУРЗ к ПЭДВ.

Литература к Гл. 6.

6.1 Platt R., Anderson B., Christofferson J., Enns J., Haworth M., Metz J., Pelletier P., Rupp R., Voss D. Low-frequency multi-gigawatt microwave pulses generated by a virtual cathode oscillator. - Applied Physics Letters 27.03. 1989, Vol. 54 Issue 13, p. 1215.

6.2 Counter-Electronics High Power Microwave Advanced Missile Project (CHAMP) Joint Capability Technology Demonstration (JCTD). Solicitation Number: BAA-08-RD-04, 16 October 2008 (Restricted Data).

6.3 Методы обеспечения стойкости перспективных систем радиорелейной, тропосферной и спутниковой связи к воздействию мощных импульсных электромагнитных помех / Воскобович Владимир Викторович — 05.12.13 — Москва, 2002.

6.4 Разработка методов оценки стойкости телекоммуникационных систем к воздействию сверхширокополосных электромагнитных импульсов / Ведмидский Александр Александрович — 05.12.13 — Москва, 2003.

6.5 Теоретические и экспериментальные методы оценки устойчивости терминалов к воздействию сверхшироко-полосных электромагнитных импульсов / Акбашев, Беслан Борисович — 05.12.13 — Москва, 2005.

6.6 Методы и средства оценки воздействия электромагнитного импульса большой энергии на телекоммуникационные сети / Якушин Сергей Павлович — 05.12.13 — Москва, 2004.

6.7 Radasky W., Savage E., Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid - Meta-R-323. Metatech report for Oak Ridge National Laboratory, 2010.

6.8 NATO AECTP-250 Leaflet 257 – High Power Microwave (HPM).

6.9 MIL-STD-461F Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 2007.

6.10 Staines G. Compact Sources for Tactical RF Weapons Application. - DIEHL Munitionssyteme. Amerem-2002, Maastricht, Nederlands, 2002.

6.11 R. Barker and E. Shamiloglu. High-Power Microwave Sources and Technologies. IEEE Press, New York, 2001.
6.12 W. Prather, C. Baum et al. Ultra-wideband Source and Antenna Research". IEEE Trans. Plasma Sci., Vol.28, pp. 1624-1630, Oct. 2000.
6.13 Многоволновые СВЧ-генераторы сверхбольшой мощности / Кошелев В.И. — 01.04.04 — Томск, 1990.
6.14 Мощные импульсные СВЧ-генераторы на основе лампы обратной волны в режиме сверхизлучения / Ельчанинов А.А. — 01.04.04 — Томск, 1990.
6.15 Генерация мощного СВЧ излучения на основе сильноточных наносекундных электронных пучков / Коровин С.Д. — 01.04.04 — Томск, 1990.
6.16 Savage E., Gilbert J., Radasky W. The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid. – Report Meta-R-320 for Oak Ridge National Laboratory, 2010.
6.17 Гуревич В. И. Проблемы стандартизации в области микропроцессорных устройств релейной защиты. - Компоненты и технологии, 2012, № 1, с. 6 - 9.
6.18 Гуревич В. И. Уязвимости микропроцессорных реле защиты. Проблемы и решения. – М.: Инфра-Инженерия, 2014. – 256 с.
6.19 Perrow C. Normal accidents. Living with high risk technologies. First ed. Princeton: Princeton University Press, 1984.
6.20 EMP Effects on Protection and Control Systems. - Schweitzer Engineering Laboratories, 2014, 31 p.
6.21 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, April 2008

7. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ МУРЗ ОТ ЭМИ

7. 1. Проблемы стандартизации МУРЗ

Стандартизация и универсализация МУРЗ является одним из важнейших направлений повышения живучести релейной защиты при воздействии ЭМИ, поскольку позволяет существенно ускорить процесс восстановления ее работоспособности после повреждения электромагнитным импульсом или другими средствами дистанционного электромагнитного поражения, а также является одним из путей повышения эффективности эксплуатации МУРЗ и в обычных условиях.

7. 1.1. Кто координирует процесс стандартизации в области релейной защиты?

Сегодня микропроцессорные устройства релейной защиты (МУРЗ) выпускаются десятками крупнейших мировых компаний, таких как ABB, Siemens, General Electric, Alstom (Areva), SEL, Nari Relays, Beckwith Electric, Schneider Electric, Cooper Power, Orion Italia, VAMP, Woodward и др., а также многочисленными компаниями в России и Украине (АББ Реле-Чебоксары, НПП «Экра», НПП «Бреслер», ЗАО «ЧЭАЗ», Радиус-Автоматика, Хартрон-Инкор, Киевприбор, РЕЛСіС, РЗА СИСТЕМЗ, Энергомашвин, НТЦ «Механотроника» и др.

Каждый из многочисленных производителей МУРЗ сам устанавливает размеры и форму для каждой выпускаемой им модели, состав и конструкцию внутренних модулей, программное обеспечение. В результате, сегодня на рынке представлены сотни вариантов МУРЗ абсолютно не совместимых друг с другом ни по аппаратной части, ни по программной. Более того, в большинстве случаев абсолютно не совместимыми оказываются и МУРЗ разных моделей или разных поколений даже одного и того же производителя.

Такое положение дел приводит к возникновению серьезных проблем, сдерживающих развитие релейной защиты. Так, например, несовместимость аппаратной части МУРЗ приводит к тому,

что приобретя единожды дорогостоящий комплект устройств релейной защиты, потребитель вынужден в течение многих лет приобретать совсем не дешевые запасные модули только у того же самого производителя, даже если их качество оставляет желать лучшего. Множество проблем порождают и тендерные закупки релейной защиты, которые практикуются сегодня в большинстве стран мира. Победа разных компаний-производителей в периодически проводимых тендерах приводит к тому, что за 10 – 15 лет в одной энергосистеме скапливаются в эксплуатации десятки самых разных моделей МУРЗ, выпущенных разными производителями, что резко увеличивает нагрузку на эксплуатирующий персонал и увеличивает количество ошибок на всех стадиях: от расчета уставок, до ввода этих уставок и проверках реле. По данным, опубликованным разными авторами, процент неправильных действий МУРЗ по причине ошибок обслуживающего персонала (так называемый «человеческий фактор») доходит до 50-70% [7.1-7.3]. Различные программные интерфейсы и полная несовместимость программного обеспечения МУРЗ не позволяет осуществить автоматизацию процесса комплексного испытания МУРЗ, который сегодня занимает много времени и сил у обслуживающего персонала и представляет собой еще одно место для возможных ошибок персонала (например, при возврате реальных уставок после испытаний) [7.4].

В связи с отсутствием стандартов, то есть, фактически, ограничительных рамок, современные тенденции развития МУРЗ продолжаются в направлении все большего их усложнения, увеличения количества реализуемых функций, использования МУРЗ для решении задач, совершенно не свойственных РЗ, например, таких, как мониторинг состояния электрооборудования, совершенно недопустимым, по нашему мнению, увеличения степеней свободы МУРЗ, к которому призывают некоторые специалисты [7.5 - 7.12]. Следует отметить, что тенденция постоянного усложнения МУРЗ наблюдается во всем мире и ею грешат практически все производители МУРЗ, ведь более сложное и более «навороченное» устройство легче рекламировать и можно продать его по более высокой цене. Однако, конечные пользователи оценивают такие тенденции в релейной защите не совсем так, как производители. Вот, например, как оценивают релейную защиту одного из ведущих мировых производителей МУРЗ российские специалисты-релейщики [7.13]:

«В терминале Siprotec 7SJ642 (Siemens) заложена неоправданная техническая и информационная избыточность. В руководстве по эксплуатации (C53000G1140C1476, 2005 г.) отмечается «простота работы с устройством с помощью интегрированной панели управления или посредством подключения ПК с системной программой DIGSI», что не соответствует действительности. Например, требуется вводить около 500 параметров (уставок), не считая внесения неизбежных изменений в матрицу сигналов, а у каждого из сигналов есть «свойства», влияющие на работу устройства (распечатанная из DIGSI матрица сигналов занимает около 100 страниц англоязычного текста). Учитывая необходимость составления заданий на наладку и протоколов проверки терминалов, где должны указываться все параметры настройки, объем документации становится неподъемным. Большой объем вводимой информации усложняет настройку. Информационная избыточность повышает вероятность ошибок, связанных с человеческим фактором. Техническая избыточность требует для работы с терминалом специалистов высокой квалификации. Документация фирмы по рассматриваемым терминалам – это тысячи страниц, но при этом зачастую нет нужной информации, встречаются ошибки».

К сожалению, такая ситуация существует на рынке МУРЗ уже многие годы и продолжает лишь усугубляться, а организации, призванные координировать деятельность в этой области (например, такие, как ВНИИР в России), не только не занимаются решением этих вопросов, но и сами способствуют усугублению проблемы, предлагая неимоверно расширять функции МУРЗ за счет навешивая на них совершенно не свойственных релейной защите функций, использовать в РЗ недерминированную логику и так называемый «искусственный интеллект». Так, в частности, предлагается придать МУРЗ функции мониторинга силового электрооборудования и прогнозирования его состояния. Предполагается, что такая РЗ будет осуществлять отключение электрооборудования по результатам оценки своих собственных прогнозов, задолго до наступления аварийного режима (так называемая «релейная защита упреждающего

действия» [7.10 - 7.12]. В этой связи возникает вопрос о том, а что же такое вообще «реле защиты», если оно может заниматься прогнозами и отключать электрооборудование до наступления аварийного режима.

Сегодня не существует узаконенного в стандартах определения даже такому базовому понятию, как «реле защиты». В различных учебниках по релейной защите разными авторами даются разные трактовки этого понятия, далеко не всегда верные и отражающие лишь субъективные взгляды их авторов [7.14]. Отсутствие стандартного определения понятию «реле защиты» способствует не только совершенно произвольной трактовке этого понятия, но, и как следствие этого, приписыванию реле защиты совершенно не свойственных ему функций, что является далеко не безобидным занятием и может привести к непредсказуемым последствиям [7.12].

Поэтому, по нашему мнению, стандартизация в области МУРЗ должна начаться с четкого и понятного определения понятию «реле защиты», которое обязательно должно быть записано в стандарте. Очевидно, что в случае принятия определения, предложенного в [7.14], ситуация существенно прояснится от того тумана, который сегодня напускается некоторыми учеными на релейную защиту и она очистится от идей и разработок, которые сами по себе весьма ценны и интересны, но не имеют ни малейшего отношения к собственно релейной защите.

7.1.2. Основные принципы стандартизации МУРЗ

Какие основные принципы должны найти отражение в будущем стандарте? По нашему мнению, это должны быть:

- запрет на использования в МУРЗ функций, не свойственных реле защиты в соответствии с узаконенным определением «реле защиты»;
- существенное ограничение количества функций в одном микропроцессорном терминале; расчет оптимального количества таких функций по критерию не только стоимости РЗ, но и ее надежности.

- отказ от использования алгоритмов с недетерминированной логикой, допускающих непредсказуемые действия релейной защиты;
- максимальное упрощение программного интерфейса на основе некоей универсальной для всех МУРЗ программной платформы (в стандарте должны быть изложены основные требования и принципы такой платформы);
- введение требований на устойчивость функционирования микропроцессорной релейной защиты в условиях преднамеренных деструктивных электромагнитных воздействий, как за счет повышения устойчивости самих МУРЗ к таким воздействиям, использования технических средств, существенно ослабляющих такие воздействия, так и за счет автоматического введения резервного комплекта РЗ при чрезвычайных ситуациях, на роль которого подходят электромеханические реле.
- введение усиленных требований по кибернетической безопасности, включая запрет на использовании технологий, при которых команды и сигналы релейной защиты могут быть перехвачены и преднамеренно искажены, например, беспроводных технологий (Wi-Fi), сетевых технологий Ethernet.

Помимо общих принципов, изложенных выше, в стандарт должны быть включены, по нашему мнению, требования к конструкции МУРЗ.

О каких требованиях идет речь?

7.1.2.1. Стандартизация внешнего исполнения МУРЗ

Как уже отмечалось выше, сегодня каждый тип МУРЗ имеет собственный корпус, существенно отличающийся от корпуса другого типа МУРЗ, иногда даже того же самого производителя, рис. 7.1. Эти отдельные МУРЗ размещаются сегодня, как правило, в релейных шкафах: по 3 – 5 штук в каждом шкафу, рис. 7.2.

Исторически сложилась ситуация [7.15], при которой сегодня мы имеем огромное количество абсолютно не взаимозаменяемых и не совместимых между собой конструктивных исполнений МУРЗ.

Рис. 7.1. Современные МУРЗ в корпусах различных типов и размеров

Потратив однажды кругленькую сумму на приобретение комплекта МУРЗ у одного из производителей, потребитель, фактически, попадает в экономическую кабалу к этому производителю на период в 10 – 15 лет, поскольку после совершения сделки для потребителя уже не имеет значения наличие нескольких разных производителей на рынке, так как он не может воспользоваться изделиями других производителей. Выбраться из этой кабалы можно только потратив еще раз не менее круглую сумму на приобретение

комплекта МУРЗ другого производителя (и, таким образом, из одной кабалы попасть в другую).

Рис. 7.2. Современный способ монтажа МУРЗ в шкафах

А что делает производитель в ситуации абсолютного монополиста? Правильно: повышает цену! Цена одного запасного модуля для МУРЗ может доходить чуть ли не до трети и даже половины цены всего весьма не дешевого МУРЗ! Поскольку потребителю некуда деваться, он покупает и по такой цене. А что происходит через 8 – 10 лет эксплуатации МУРЗ? А вот что: производитель за это время освоил уже несколько новых конструкций и ему становится просто не выгодным содержать производственные мощности для выпуска запасных модулей для старых реле и он просто прекращает их выпускать. Что в такой ситуации вынужден делать потребитель? Правильно: выбросить старый МУРЗ, даже если в нем вышел из строя всего лишь один из модулей (печатные платы современных МУРЗ выполнены по технологии, не предусматривающей их ремонт), и раскошелиться на приобретение нового. Таким образом, отсутствие

стандарта на конструкцию МУРЗ перерастает в серьезную экономическую проблему, сдерживающую развитие и модернизацию релейной защиты.

По нашему мнению, МУРЗ следующего поколения должны производиться в виде отдельных функциональных модулей (печатных плат), унифицированных по размерам и снабженных унифицированными разъемами, (соединителями).

В этом случае для такого набора плат станут не нужными (во всяком случае, в большинстве случаев, встречающихся в электроэнергетике) отдельные корпуса.

Каждый МУРЗ может быть образован отдельной горизонтальной секцией в шкафу с направляющими под печатные платы, с индивидуальной дверцей и с задней стенкой с разъемами и клеммами для подключения внешних кабелей.

Сам релейный шкаф должен быть выполнен по специальной технологии, предназначенной для защиты его содержимого от электромагнитных воздействий. Сегодня существуют технологи (специальные шкафы, электропроводные прокладки и смазки, фильтры и т.п.), которые могут существенно ослабить влияние внешних электромагнитных излучений в широком спектре частот на высокочувствительную аппаратуру типа МУРЗ. Такие шкафы выпускаются сегодня такими компаниями, как: R.F. Installations, Inc.; Universal Shielding Corp.; Eldon; Equipto Electronics Corp.; European EMC Products Ltd; Amco Engineering, и многими другими.

7.1.2.2. Стандартизация функциональных модулей МУРЗ

Сегодня, модули, из которых состоят МУРЗ, далеко не всегда представляют собой отдельные функциональные модули, а часто имеют вид «сборной солянки», когда на одной печатной плате размещены разные функциональные блоки [7.16]. Для реализации идеи универсализации МУРЗ такая конструкция не подходит, поэтому каждая печатная плата будущих МУРЗ должна представлять собой однофункциональный модуль, например: модуль центрального процессора, модуль источника питания, модуль аналоговых входов, модуль логических входов, модуль выходных реле.

При таком конструктивном выполнении МУРЗ на рынке появились бы новые «игроки», одни из которых специализировались бы

на выпуске модулей аналоговых входов с трансформаторами тока и напряжения, другие – на выпуске материнской платы, третьи – на модулях цифровых входов, четвертые – на выпуске шкафов разной емкости: от небольших подвесных, до полногабаритных напольных. Потребитель мог бы компоновать свой МУРЗ из модулей различных производителей, точно так, как это происходит сегодня с персональными компьютерами, с учетом стоимости и качества этих модулей. При этом были бы решены не только очень многие из существующих сегодня проблем МУРЗ, но и была бы существенно снижена стоимость релейной защиты. Последнее позволило бы устанавливать два комплекта идентичных защит вместо одного для повышения надежности и использовать второй комплект как резервный, автоматически запускаемый в работу по сигналу "watchdog" поврежденного основного МУРЗ. Можно было бы отказаться от использования индивидуального источника питания для каждого МУРЗ и использовать один сдвоенный комплект питания повышенной мощности и надежности на весь шкаф. Можно было бы установить в таком шкафу много разных сервисных модулей, повышающих надежность работы МУРЗ.

Рис. 7.3. Многостраничные фолианты с описанием МУРЗ, предназначенные для потребителя

Значительно упростилась бы работа обслуживающего персонала, то есть служб релейной защиты, поскольку теперь им не нужно было бы изучать толстенные фолианты (рис. 7.3) каждого из установленных типов МУРЗ и разбираться с особенностями каждого из них. Кроме существенного облегчения работы с МУРЗ и сокращением времени освоения новых защит, существенно снизился бы

процент ошибок, вызванных так называемым «человеческим фактором».

7.1.2.3. Стандартизация программного обеспечения МУРЗ

Программное обеспечение МУРЗ должно быть реализовано, по нашему мнению, также на принципах, хорошо зарекомендовавших себя в персональных компьютерах, то есть, должна быть базовая программная оболочка, аналогичная Windows (но существенно более простая, конечно) и набор прикладных программ и библиотек, предназначенных для конкретных типов защит. При наличии универсальной программной платформы и унифицированной блочной конструкции МУРЗ неизбежно появился бы и рынок прикладных программ для различных типов защит. Более того, можно было бы добиться и того, чтобы интерфейсы этих прикладных программ были бы также стандартизированы с тем, чтобы потребителю не приходилось каждый раз при покупке нового МУРЗ или новой программы переучиваться и изучать с нуля новый программный интерфейс, как это происходит сегодня.

7.1.2.4. О необходимости стандартизации испытаний МУРЗ

Испытания МУРЗ при вводе в эксплуатацию и в процессе эксплуатации представляют собой набор достаточно сложных и ответственных операций от четкости и безошибочности выполнения которых зависят не только затраты времени на испытания, но во многом зависит правильность действия релейной защиты. Последнее обстоятельство обусловлено тем, что в процессе испытаний часто приходится изменять уставки реле или блокировать конкурирующие функции, а затем возвращать их. Проверки защитных характеристик сложной формы (в частности, характеристик дистанционной защиты) современных многофункциональных МУРЗ возможны лишь с использованием современных испытательных комплексов, которые сами по себе очень сложны. Необходимость правильной стыковки сложных МУРЗ со сложными испытательными комплексами представляет собой отдельную проблему [7.4], которая подробно рассмотрена в [7.14].

7.1.2.5 Основные принципы конструирования МУРЗ – основа будущего стандарта

Итак, основные принципы, которые должны быть заложены, по нашему мнению, в будущий стандарт под условным наименованием: «Принципы конструирования микропроцессорных устройств релейной защиты. Основные требования», таковы:

1. Функциональные блоки МУРЗ должны быть физически четко разделены и хаотический принцип размещения этих функциональных блоков на печатных платах, имеющий место сегодня [7.15] должен быть заменен упорядоченным размещением, оговоренным специальным стандартом. К примеру: такие функциональные модули, как, источник питания, модуль входных трансформаторов тока и напряжения с элементами предварительной обработки сигналов, модуль цифровых входов, модуль выходных реле, модуль центрального процессора и т.д. должны быть выполнены на отдельных печатных платах стандартных размеров, снабженных универсальными разъемами.

2. Отдельные устройства релейной защиты энергетических объектов должны производиться и продаваться не виде отдельных, изделий, снабженных индивидуальными корпусами разных размеров и формы, а виде отдельных универсальных печатных плат (модулей), из которых потребитель может собрать МУРЗ требуемой конфигурации. Эти платы (модули) должны быть предназначены для простой установки (путем введения по направляющим до состыковки с разъемом кросс-платы) в металлические шкафы, снабженные отдельными отсеками с отдельными дверцами. Металлические шкафы должны быть выполнены по технологии, предусматривающей защиту их содержимого от внешних электромагнитных излучений.

3. Функции МУРЗ должны быть ограничены только задачами релейной защиты и никакими другими. Количество функций в одном модуле должно быть оптимизировано по показателям «стоимость» и «надежность» и ограничено стандартом.

4. Программное обеспечение для компьютера, предназначенное для работы с МУРЗ должно состоять из стандартной базовой оболочки и набора различных прикладных программ и библиотек, совместимых с общей базовой оболочкой.

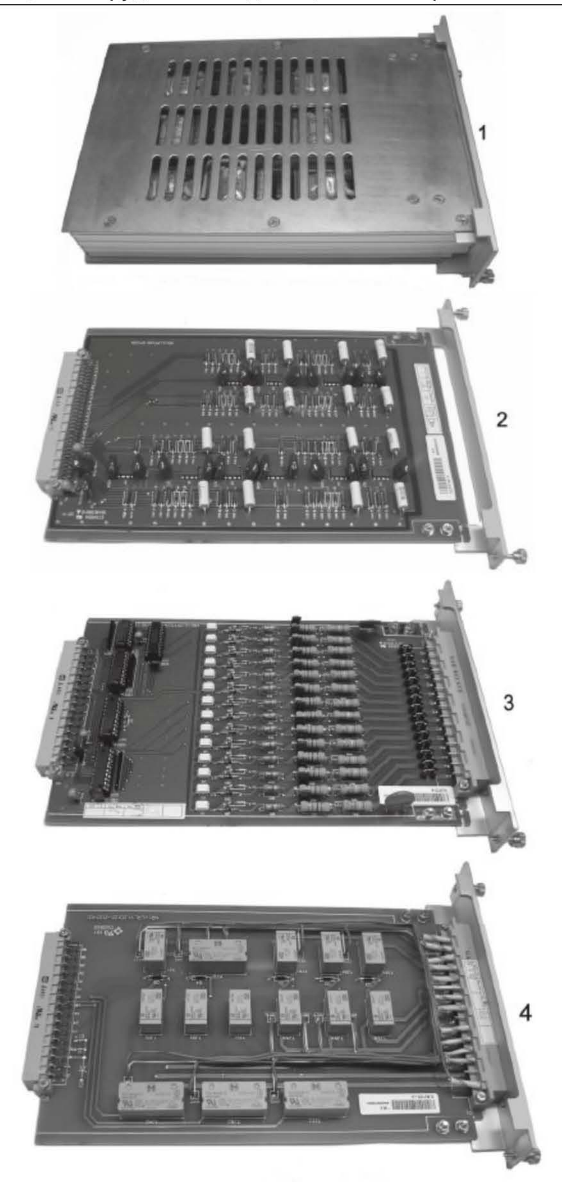
5. Питание всех модулей в шкафу должно осуществляться от двух источников повышенной надежности, соединенных между собой как основной и резервный.

Возможна ли, с технической точки зрения, реализация предлагаемой концепции построения МУРЗ?

Как отмечалось выше, большинство из имеющихся сегодня на рынке МУРЗ не имеют строго разделенного по функциям набора модулей, а их конструкция напоминает скорее «сборную солянку», когда на одной печатной плате блок центрального процессора может соседствовать с импульсным источником питания, рис. 7.4.

Рис. 7.4. Объединенный модуль МУРЗ, на котором центральный микропроцессор соседствует с источником питания и выходными реле

Однако, проведенный нами анализ многих типов самых современных МУРЗ ведущих мировых производителей, позволил все же найти устройства, идеально удовлетворяющие уже сегодня сформулированному выше требованию в части конструктивного исполнения [7.16].


1
2
3
4

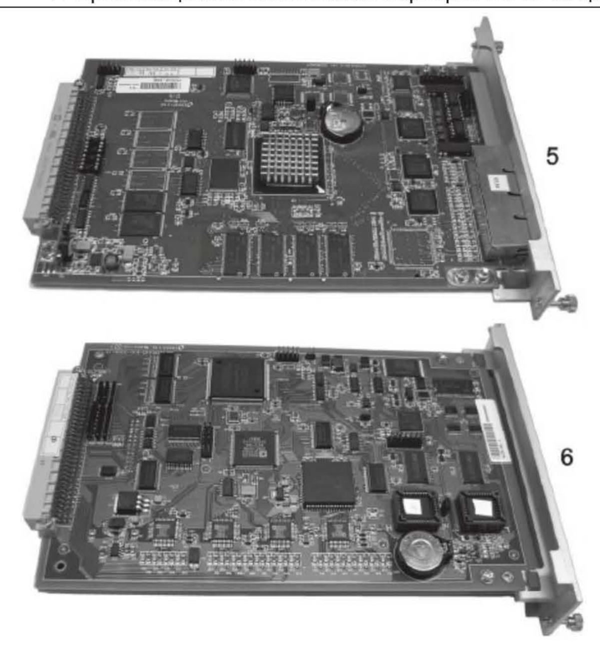


Рис. 7.5. Набор универсальных функциональных модулей (220 x 145 мм), выполненных на отдельных печатных платах, из которых состоят различные МУРЗ, производства компании Nari-Relays: PCS-931 (дифференциальная защита линий), PSC-902 (дистанционная защита), и др. 1 – модуль входных трансформаторов тока и напряжения; 2 – узкополосный фильтр (антиалиазинговый фильтр); 3 – модуль цифровых входов; 4 – модуль выходных реле; 5 – модуль оптической связи; 6 – модуль центрального процессора.

Такими устройствами являются МУРЗ серии 900 известной Китайской компании Nari-Relays с их универсальными модулями, используемыми в защитах разного типа, рис. 7.5. Эти модули полностью готовы к использованию и не требуют никакой предварительной подготовки (кроме программного конфигурирования функций защиты, разумеется). Не требуется и никакой наладки МУРЗ после его сборки, которая заключается лишь в установке печатных плат, изображенных на рис. 7.5 (в реальный комплект входит еще и плата

источника питания, который не нужен в нашей концепции и поэтому не показан) в размеченные направляющие корпуса (в нашем случае это будет отсек шкафа). На сборку такой сложной защиты, как дистанционная, из 7 отдельных модулей, поставляемых в картонных коробках, и включение реле требуется не более 10-15 минут, после чего можно начинать ввод уставок. Совершенно очевидно, что рядовой инженер-релейщик, не имеющий специальных знаний в области микропроцессорной техники, с легкостью справится со сборкой реле защиты из таких универсальных блоков непосредственно на месте его установки.

В принципе, уже сегодня ничего не мешает началу воплощения предлагаемой концепции на территории отдельной страны. Приобретая на первых порах наборы универсальных модулей Nari-Relays (с разными алгоритмами, записанными в EEPROM и разными наборами входных трансформаторов), и освоив производство шкафов под них, даже небольшая компания способна уже сегодня выйти на рынок МУРЗ, предложив потребителю новую концепцию дешевой и надежной релейной защиты, оснащенной резервными блоками-модулями.

Какие преимущества сулит предлагаемый путь развития МУРЗ?

Для потребителя:

- значительное снижение стоимости МУРЗ при покупке;
- возможность компоновать МУРЗ из отдельных модулей, различных производителей, наиболее полно удовлетворяющих потребности эксплуатирующей организации с точки зрения наиболее оптимального баланса между качеством и стоимостью;
- возможность создания оптимального ЗИПа модулей МУРЗ;
- снижение актуальности проблемы пониженной надежности МУРЗ за счет быстрой и свободной замены на месте вышедших из строя дешевых модулей, за счет установки резервных модулей, автоматически вводимых в работу при повреждении основных; исключение необходимости в ремонте вышедших из строя модулей МУРЗ;
- возможность ухода от привязки к монополисту-производителю, единожды продавшему МУРЗ;

- усиление конкуренции между производителями за счет появления на рынке новых «игроков» - малых и средних компаний, специализирующихся на выпуске лишь отдельных видов модулей, а не комплектных МУРЗ;
- упрощение испытаний МУРЗ и снижение влияния «человеческого фактора»;
- значительное упрощение работы с программным обеспечением, возможность выбора наиболее подходящей и удобной прикладной программы (интерфейса), возможность безболезненной замены прикладных программ (интерфейсов) для одного и того же МУРЗ;
- ускорение технического прогресса в области МУРЗ, без усложнения их эксплуатации и без возникновения дополнительных проблем у потребителя при каждом переходе на новое поколение устройств
- снижение затрат на обновление МУРЗ, поскольку обновлять весь МУРЗ каждые 10-15 лет, как это часто происходит сегодня, не обязательно. Достаточно обновить его отдельные модули. Более того, обновлять материнскую плату можно даже чаще, чем это делается сейчас, ускоряя технический прогресс в этой области.

Для производителя:

- отсутствие необходимости в выпуске устаревших модулей, необходимых для поддержания эксплуатации старых моделей МУРЗ;
- отказ от пожизненного бесплатного ремонта МУРЗ;
- значительный рост потребления отдельных модулей;
- появление нового рынка прикладных программ (интерфейсных оболочек);
- возможность специализации на производстве каких-то отдельных, наиболее выгодных для данного производителя, видов модулей;
- возможность участия в данном бизнесе малых и средних компаний, не имеющих достаточных ресурсов для разработки и производства комплектных МУРЗ;

- конкурентное преимущество национальных производителей, первыми начавшими производство МУРЗ в виде модулей на территории отдельной страны, перед иностранными.

Концепция построения МУРЗ из набора универсальных блоков-модулей ни в коей мере не препятствует их совершенствованию и развитию, использованию новых принципов построения.

Рис. 7.6 Модуль аналоговых входов традиционной конструкции с трансформаторами тока

Например, очень перспективной, по нашему мнению, является замена общепринятых сегодня трансформаторов тока в модуле аналоговых входов, рис. 7.6 миниатюрными шунтами, рис. 7.7. Миниатюрные шунты выполнены в виде перемычек длиной 5 мм между токовыми входами непосредственно на силовом разъеме. Весь этот разъем разбит на четыре группы по три вывода в каждой. Центральный вывод каждой группы общий и для цепи тока и для цепи напряжения. Левый крайний вывод – токовый, правый крайний – напряжения. То есть, каждый из четырех измерительных каналов может быть использован или как аналоговый вход тока, или как аналоговый вход напряжения.

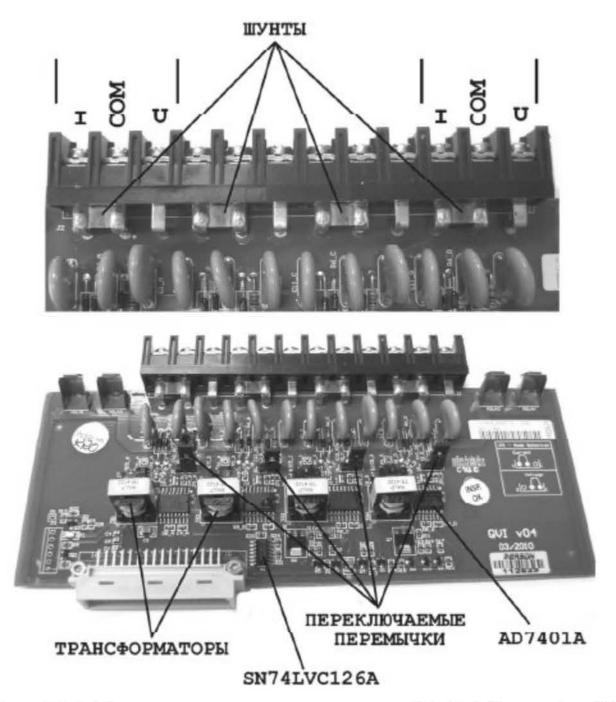


Рис. 7.7. Модуль аналоговых входов Digital Recorder RPV-311 (RT Measurement Technologies GbmH) размерами 190x75 мм

Каждый из этих входов должен быть дополнительно сконфигурирован как вход тока или вход напряжения с помощью переключаемых перемычек на плате. Несмотря на миниатюрные размеры, шунты обладают очень хорошими параметрами:

- номинальный ток 5А
- длительная перегрузка – 10А
- кратковременная перегрузка (2 с) – 100 А
- диапазон входных токов 0.25А – 100 А
- точность – 0.1% от полной шкалы
- сопротивление – 3 мОм, нагрузка на внешний ТТ – меньше 0.1 ВА

В этом модуле входные аналоговые сигналы (и ток и напряжение) преобразуются в милливольты, которые затем переводятся в высокочастотный (до 20 Мгц) цифровой сигнал посредством аналого-цифровых преобразователей типа AD7401A с высоковольтной изоляцией входа от выхода (по данным производителя – выдерживаемое одноминутное напряжение 5 кВ), передается далее через высокочастотные трансформаторы на ферритовых сердечниках, нормализуются с помощью счетверенного набора логических элементов типа SN74LVC126A и поступает на выходной разъем.

Таким образом, принятые компаний RT Measurement Technologies GbmH технические решения позволили создать универсальный (ток/напряжение) модуль аналоговых сигналов, отличающийся своей простотой и малыми размерами, то есть сделать еще один шаг навстречу обсуждаемой концепции универсального набора модулей для построения различных типов реле защиты.

Совершенно очевидно, что все изложенное выше является лишь наброском некоторых общих принципов будущего стандарта. К реальной работе над этим стандартом должен быть привлечен широкий круг специалистов, представляющих и ученых, и будущих производителей МУРЗ, и будущих потребителей, и представителей проектных организаций. Отсутствие, сегодня, таких стандартов, то есть каких бы то ни было ограничивающих рамок и направлений развития МУРЗ уже сегодня приводит к значительным экономическим потерям, а в ближайшем будущем может привести к полному хаосу в этой области.

7.2. Основные принципы стандартизация испытаний МУРЗ

Стандартизация испытаний МУРЗ – еще одно важнейшее направление сокращения времени восстановления релейной защиты после замены МУРЗ, пораженного электромагнитным импульсом или другими средствами дистанционного электромагнитного поражения. После установления факта воздействия ПЭДВ на энергосистему (подстанцию) и ее аварийного отключения, перед возвратом в рабочее состояние должна быть проверена исправность МУРЗ, возвращаемых в работу. Одной из проблем МУРЗ является сложность проверки их исправности, что неизбежно сказывается на времени восстановления электроснабжения.

Исправность устройств релейной защиты обычно принято проверять на тех конкретных уставках, которые будут использоваться в дальнейшем при реальной работе реле в данной конкретной точке сети. При изменении уставок в процессе эксплуатации реле требовалось повторная проверка работоспособности реле с этими новыми уставками. Во времена электромеханических реле защиты это было вполне оправданной мерой, так как переход с одной уставки на другую осуществлялся путем механического перемещения внутренних элементов реле или переключения отпаек встроенных трансформаторов и.т.п. При изменении настроек таких реле вполне могло оказаться, что внутренние цепи реле, подключенные к новой отпайке трансформатора не исправны (обрыв провода, нарушение контакта, поврежденная изоляция и т.п.) или, что в новом положении механических элементов реле нарушается его балансировка, появляется «затирание» и т.п. неприятности. Поэтому, нормальная работоспособность электромеханического реле с одним набором уставок еще не гарантировала его работоспособности с другими уставками.

В микропроцессорных реле защиты (МУРЗ) переход с одного набора уставок на другой не сопровождается физическими изменениями в его внутренней структуре. Независимо от конкретных уставок и режимов работы, в МУРЗ работают одни и те же входные и выходные цепи, одни и те же логические элементы, тот же самый процессор, тот же самый источник питания и т.д. Даже включение или отключение отдельных функций МУРЗ не связано с изменениями физического состояния его цепей. Проверка же правильности выбора логики защиты и правильности расчета уставок для конкретных условий конкретной сети – это совсем другая задача, которая не имеет отношения к проверке исправности реле и решается не персоналом, эксплуатирующим реле и отвечающем за его исправность, а инженерной службой, отвечающей за расчеты уставок и выбор внутренней логики работы реле. Да и не возможно в процессе тестирования исправности реле смоделировать все реальные ситуации и все возможные комбинации факторов, действующих в реальной сети. Выявление таких ситуаций не является целью проверки исправности реле защиты. Более того, можно показать, что отказ от проверки реле с использованием расчетных уставок является положительной мерой, снижающей риск неправильных действий защиты вследствие так называемого «человеческого фактора» (при-

чины почти 50% неправильных действий защиты). Дело в том, что в многофункциональных микропроцессорных защитах уставки для конкретных условий работы выбираются таким образом, что проверить определенные функции реле можно только при загрублении или полном отключении другой, конкурирующей функции. Не возврат такой загрубленной или отключенной функции в исходное положение после окончания тестирования реле часто является причиной неправильных действий защиты в аварийных режимах. Аналогичный подход к проблеме испытаний реле защиты принят и в [7.17]. В этом документе, имеющем статус стандарта, все испытания реле разделены на два вида: калибровочные испытания (предназначенные для проверки уставок и конфигурации реле) и функциональные. Если для функциональных испытаний установлена периодичность один раз в 4 года *для всех типов реле* (включая электромеханические и микропроцессорные), то для калибровочных испытаний установлена периодичность один раз в 4 года *только* для электромеханических реле. Периодическая калибровка (то есть проверка уставок) микропроцессорных реле защиты вообще не предусмотрена.

7.2.1. Новый взгляд на проблему

На основании изложенного выше, можно сформулировать некоторые принципы, которые могут быть приняты при тестировании МУРЗ:

1. Для подтверждения исправности сложных многофункциональных МУРЗ при вводе их в эксплуатацию, после ремонта или в процессе периодических испытаний совершенно не обязательно проводить их тестирование именно на тех уставках, при которых реле будет в дальнейшем работать в данной конкретной сети.

2. Для проверки исправности МУРЗ достаточно проверить их правильное функционирование лишь в некоторых, *заранее заданных*, наиболее критичных точках характеристики; в некоторых, *заранее заданных,* наиболее сложных (комбинированных) режимах работы, включая динамические режимы работы с *заранее заданными* переходными процессами, характерны-

ми для типовых электрических сетей (но не обязательно для данной конкретной сети).

Рис. 7.8. Набор индуктивностей фирмы General Electric для проверки электромеханических реле защиты

Рис. 7.9. Испытательная установка типа TURH-20 (ASEA) для проверки электромеханических реле защиты содержащая наборы индуктивностей и активных сопротивлений

Такие испытания должны охватывать все физические входы и выходы реле. После окончания проверки реле и подтверждения его исправности все тестовые уставки должны быть автоматически заменены заранее приготовленным набором (файлом) реальных расчетных уставок.

3. Такое тестирование микропроцессорной защиты в наиболее сложных режимах работы позволит, по нашему мнению, значительно лучше проверить исправность МУРЗ, нежели ограниченная проверка в очень ограниченных пределах конкретных уставок, при которых МУРЗ будет в дальнейшем функционировать.

4. Комплексная проверка МУРЗ при вводе его в эксплуатацию в наиболее тяжелых для него режимах работы позволяет исключить дополнительные проверки работоспособности МУРЗ при каждом изменении уставок в процессе эксплуатации.

Сформулированные выше принципы позволяют по-новому взглянуть на проблему тестирования МУРЗ.

Можно предположить, что первые приспособления для проверки реле защиты появились практически одновременно с самими реле защиты. Естественно, они были такими же примитивными, как и сами реле защиты. На первых порах это были просто калиброванные катушки индуктивности, рис. 7.8, и реостаты.

По мере совершенствования реле, усложнялись и испытательные установки для их проверок. Появились испытательные стенды (рис. 7.9) содержащие наборы индуктивностей и активных сопротивлений, с помощью которых уже можно было задавать углы между током и напряжением в широком диапазоне и проверять достаточно сложные электромеханические реле.

В разных энергосистемах были установлены различные сроки периодических проверок релейной защиты (один раз в 2 – 3 года), но они, обычно, соблюдались неукоснительно.

С появлением на рынке микропроцессорных устройств релейной защиты (МУРЗ) ситуация кардинально изменилась. Производители этих устройств заявили, что микропроцессорные реле якобы не нуждаются в периодических проверках потому, что имеют мощную встроенную систему самодиагностики. Эта особенность МУРЗ фигурировала в рекламных проспектах чуть ли не как главное их пре-

имущество перед электромеханическими и аналоговыми электронными реле. Мощная рекламная компания, развернутая производителями МУРЗ, сыграла свою роль. Многие специалисты релейной защиты безоговорочно поверили в этот рекламный трюк, не имея возможности на практике проверить достоверность этого утверждения, хотя было совершенно очевидно, что невозможно создать тестовую систему на базе внутреннего микропроцессора МУРЗ, которая проверяла бы физическую исправность многих тысяч электронных компонентов. Да и функционально невозможно проверить исправность, например, блока входов или блока выходов без включения этих блоков и проверки реакции реле на подачу на них сигналов. На практике оказывается, что большинство МУРЗ попросту не замечают замену целой печатной платы одного вида на плату другого вида, не совместимой с текущими уставками реле. Об этом и о других рекламных трюках, связанных с «самодиагностикой» МУРЗ уже упоминалось ранее в многочисленных публикациях автора на эту тему.

В отличие от производителей МУРЗ, производители тестовых систем релейной защиты (ТСКЗ) всегда утверждали, что все реле защиты должны обязательно проходить периодические проверки, включая также и МУРЗ, поскольку так называемой «самодиагностикой» в них охвачены не более 15% программного обеспечения и «железа».

Рис. 7.10. Современные компьютеризированные тестовые системы для испытания многофункциональных микропроцессорных защит

Несмотря на утверждения производителей МУРЗ о нецелесообразности периодических проверок защит, фирмы-производители ТСРЗ продолжали, не переставая, интенсивно разрабатывать и выбрасывать на рынок все новые и новые тестовые системы.

7.2.2. Современные тестовые системы для реле защиты

Поскольку принципы построения МУРЗ сегодня стали общими для большинства фирм-производителей, то, естественно и предлагаемые сегодня на рынке тестовые системы различных фирм также весьма похожи друг на друга, и не только по внешнему виду, рис. 7.10, но и по своим характеристикам. ТСРЗ сегодня – это полностью компьютеризированные устройства, не содержащие на лицевой панели никаких органов управления, кроме гнезд для подключения внешних проводов и разъема RS232 для подключения компьютера. Стоимость таких ТСРЗ составляет десятки тысяч долларов.

Такие системы предназначены для проведения испытаний трех групп: статических (steady state tests), динамических (dynamic tests) и переходных процессов (transient tests). Первая группа испытаний предполагает проверку базовых уставок срабатывания реле и является как бы предварительным испытанием реле. Вторая группа испытаний предназначена, в основном, для проверки поведения сложных защит, таких как дистанционные или дифференциальные, на различных участках характеристик и зон защиты при изменении входных параметров (ток, напряжение, угол) во времени. Третья группа испытаний предполагает инжекцию во входные цепи реле файлов переходных процессов в формате COMTRADE, извлеченных из регистрирующих устройств, записавших реальный переходной процесс короткого замыкания в сети, или файлов в том же формате, построенных искусственно с помощью специальных программ. Результаты испытаний формируются в базу данных, реализованную, как правило, на основе Sybase SQL Anywhere и автоматически оформляются в виде стандартного протокола, который может быть переслан на принтер. Изготовители ТСРЗ предлагают, обычно, наборы тестовых процедур (библиотеки) в виде макросов для различных видов испытаний и даже для некоторых распространенных типов реле.

7.2.3. Проблемы современных ТСРЗ

Современные ТСРЗ обладают поистине супергибкостью и широчайшими функциональными возможностями. Эти ТСРЗ позволяют симулировать практически любые встречающиеся на практике условия работы реле защиты, включая создание под собственные требования искусственных COMTRADE файлов; искусственное искажение формы кривой тока; симуляция гармоник; смещение синусоиды тока относительно оси (симуляция апериодической составляющей); симуляция ответной реакции выключателя; автоматическое построение самых сложных полигональных характеристик дистанционных защит; синхронизация дифференциальных защит через спутники и т.п. Такие супервозможности современных ТСРЗ обуславливают наличие и оборотной стороны медали: необходимости вводить сотни параметров в десятки таблиц для выполнения каждого отдельного испытания реле. При этом встроенные библиотеки тестовых процедур на практике мало помогают, так как не освобождают от необходимости заполнения многих таблиц. К этому следует добавить не меньшую гибкость и универсальность испытуемого объекта (МУРЗ), также требующего введения огромного количества параметров из десятков выпадающих меню и таблиц. Малейшее несоответствие между собой настроек МУРЗ и ТСРЗ приводит к неправильным результатам. Причем, далеко не всегда можно понять, что полученные результаты неверны. И даже в тех случаях, когда ошибка очевидна (например, полученная характеристика реле не соответствует теоретической), очень сложно определить, где именно допущена ошибка: в настройках МУРЗ или в настройках ТСРЗ. На собственном опыте автор может подтвердить, что поиск ошибки такого рода чрезвычайно сложен и занимает много усилий и времени. Не менее сложна работа с моделью электрической сети (Power System Model), применяемой в ТСРЗ некоторых типов, для проверки дистанционных защит. Для настройки параметров ТСРЗ в этом режиме необходимо знание множества параметров реальной электрической сети, которые необходимо занести со специальными коэффициентами во множество таблиц. Технику и даже инженеру службы релейной защиты многие из этих параметров реальной сети и применяемых коэффициентов часто не извест-

ны, что требует участия в процедуре проверки реле инженеров из других служб энергосистемы.

7.2.4. Предлагаемое решение проблемы

Психологами давно установлено, что чем большим количество кнопок и рычажков (реальных или виртуальных, то есть программных) должен манипулировать оператор, тем ниже эффективность взаимодействия человека с такой техникой. Многие функции и возможности такой «навороченной» техники просто выпадают из человеческого восприятия. Как же совместить универсальность и широчайшие функциональные возможности ТСРЗ с реальными возможностями среднего техника или инженера службы релейной защиты, нуждающегося в быстрой и точной проверке ограниченного количества типов реле? Преодолевая огромные сложности, разрабатывать и отлаживать собственные процедуры и создавать на их основе собственную библиотеку макросов, как это предусмотрено производителями ТСРЗ? У нас имеются предложения по более радикальному решению этой проблемы:

1. Современные микропроцессорные ТСРЗ последнего поколения технически не целесообразно и экономически не оправданно использовать для тестирования простейших электромеханических реле, таких как реле тока и напряжения (например, типа РТ-40 или РН-54, как это предусмотрено производителями Российского ТСРЗ типа РЕТОМ-51). Для этих целей значительно эффективнее использование более простых тестовых систем. Не имеет никакого смысла разработка тестовых процедур для компьютерного автоматизированного тестирования таких реле, если только речь не идет об испытании сотен одинаковых реле в процессе их производства.
2. Использование в современных микропроцессорных ТСРЗ последнего поколения встроенных библиотек тестовых процедур, требующих внесения большого количества параметров и знания множества коэффициентов, можно признать целесообразным только для сложных электроме-

ханических защит старого типа (например, дистанционных защит типа LZ-31).

3. Для тестирования современных сложных многофункциональных МУРЗ должна быть разработана общая для всех типов ТСРЗ программная платформа, требования к которой должны быть узаконены международным стандартом. Примером такой общей программной платформы является общеизвестная Sybase SQL Anywhere, которая широко используется для создания базы данных в различных устройствах сбора и обработки данных, симуляторах, испытательных установках различных изготовителей. Другим примером является универсальный формат COMTRADE, который используется во всех типах микропроцессорных регистраторов аварийных режимов и, собственно, во всех типах ТСРЗ для симуляции переходных режимов.
4. Прикладные программы для работы с ТСРЗ различных типов могут иметь совершенно разные интерфейсы, но все они должны быть выполнены на общей стандартной программной платформе.
5. Производители МУРЗ должны снабжать свои защиты двумя компакт дисками. На одном из них под соответствующими номерами должны быть записаны полные наборы уставок для специфических режимов работы защит, или для характерных точек характеристики, или для типовых примеров электрических сетей. На втором, под номерами, соответствующими наборам уставок защиты, должны быть записаны полные наборы уставок для ТСРЗ и схемы внешних подключений МУРЗ к выходам и входам ТСРЗ.
6. Эффективное использование современных ТСРЗ для тестирования современных многофункциональных МУРЗ обеспечивается, по нашему мнению, только в том случае, если вся процедура тестирования сведется к загрузке в МУРЗ набора уставок номер XX1, загрузке в ТСРЗ набора уставок номер YY1, подключению МУРЗ к ТСРЗ и … приготовлению порции кофе.

Таким образом, предлагаемый набор мероприятий по унификации программной платформы современных микропроцессорных

ТСРЗ последнего поколения позволит организовать работу по тестированию современных многофункциональных МУРЗ совершенно по-новому. Это, по нашему мнению, снимет массу технических и психологических барьеров, и будет способствовать значительному сокращению времени проверки исправности МУРЗ, причем, как при воздействии ПЭДВ, так и в обычных режимах эксплуатации релейной защиты.

7.3. Создание запасов сменных модулей электронной аппаратуры – как средство повышения живучести энергосистемы

7.3.1. Оптимизация запасов сменных модулей электронной аппаратуры

Одним из эффективных путей повышения живучести энергосистемы является быстрое восстановление поврежденных устройств с использованием запасных частей, инструментов и принадлежностей (ЗИП). Однако, создание запасов ЗИП требует значительных денежных средств, особенно в случае сложнейших электронных микропроцессорных систем защиты, автоматики и управления, широко применяющихся в энергосистемах. Поэтому, во всем мире уже давно занимаются поиском оптимальных запасов ЗИП, позволяющих сочетать требуемую надежность этих систем при минимуме затрат.

Создание оптимальных запасов ЗИП – общая проблема, хорошо известная во многих отраслях техники, которая на сегодняшний день хорошо проработана теоретически с использованием различных математических методов оптимизации [7.18 – 7.25]. Известные методы оптимизации запасов ЗИП основаны на анализе статистики отказов элементов, сменных модулей или комплектных изделий. То есть, количество необходимых комплектов ЗИП рассчитывают исходя из того факта, что отказы электронной аппаратуры являются одиночными случайными событиями, происходящими с определенной частотой, подчиняющейся статистическим законам распределения случайных величин. Необходимость увеличения количества комплектов ЗИП с целью обеспечения восстановления работоспособности оборудования после воздействия ЭМИ ЯВ не вызывает сомнения. Но как именно его увеличивать? Совершенно очевидно, что в случае воздействия ЭМИ ЯВ на энергосистему произойдут

одновременные массовые отказы электронной аппаратуры, не подчиняющиеся никаким статистическим законам. Кроме того, обычный, достаточно длительный процесс заказа и получения новых комплектов ЗИП для пополнения хранящихся запасов после израсходования заготовленных ранее комплектов, непригоден в рассматриваемом случае. Поэтому простое увеличение складских запасов ЗИП в полтора-два раза (как это иногда практикуется не очень дальновидными руководителями) не решает проблемы, а такое увеличение этих запасов, при котором ЗИПом будет обеспечена абсолютно вся электронная аппаратура, находящаяся в эксплуатации – просто не реально по экономическим соображениям. Поэтому, для расчета оптимального комплекта ЗИП должен использоваться совершенно другой подход.

Предлагаемый метод базируется на трех основных принципах:

1. Не все электронные устройства должны снабжаться комплектами ЗИП, а лишь некоторые из них, определенные как критически важные устройства (КВУ), без которых в принципе невозможно даже частичное функционирование электроэнергетических объектов, среди которых, в свою очередь, должны быть выбраны лишь критически важные объекты (КВО) для энергосистемы.
2. Для выбранных КВУ должны быть созданы полные, а не частичные комплекты ЗИП.
3. Запасы ЗИП КВУ должны быть созданы в дополнение и вне связи с запасами ЗИП, хранящихся на складах.

Таким образом, оптимизация запасов ЗИП в рассматриваемом случае сводится лишь к расчету количества КВУ, необходимых для комплектации КВО в конкретной энергосистеме.

7.3.2. Проблема хранения запасов ЗИП

Проблема хранения запасов ЗИП требует решения двух задач: где хранить ЗИП и как его хранить.

Сегодня во многих энергосистемах комплекты ЗИП хранятся на складах, часто значительно удаленных от энергетических объектов, откуда их получают при необходимости ремонтные службы или

непосредственно службы, занимающиеся эксплуатацией. При необходимости восстановления КВУ после воздействия на энергосистему ЭМИ ЯВ возникает проблема экстренной доставки критически важных грузов на критические важные объекты, поскольку под воздействием мощного электромагнитного импульса с большой вероятностью будут выведены из строя микроконтроллеры, управляющие работой современных транспортных средств.

Для систем электросвязи в соответствии с [7.19] используется двухуровневая система ЗИП, включающая комплекты «ЗИП-0» и «ЗИП-Г». Комплект ЗИП-0 является неотъемлемой частью устройства (в рассматриваемом случае КВУ) и должен находиться на месте эксплуатации устройства (в нашем случае на КВО). Комплекты ЗИП-Г (групповые) используются для пополнения комплектов ЗИП-0 и хранятся в крупном центре технического обслуживания (или на складе). Комплекты ЗИП-0 и ЗИП-Г должны быть проверены и испытаны перед передачей на хранение.

Такой подход к организации хранения ЗИП электронной аппаратуры при необходимости восстановления энергосистемы после воздействия ПЭДВ полностью оправдан и является, по нашему мнению, максимально эффективным также и в электроэнергетике, поскольку устраняет проблему экстренной доставки ЗИП на КВО для восстановления КВУ. Хранение ЗИП КВУ непосредственно на месте эксплуатации КВУ не требует решения этой проблемы. Еще одна проблема может быть решена при такой организации хранения ЗИП КВУ: проблема их конфигурирования и настройки перед установкой в аппаратуру, что требует значительного времени, участия высококвалифицированного персонала, использования специальной электронной аппаратуры и компьютеров (которые также могут быть повреждены). В качестве примера такого вида КВУ могут служить современные микропроцессорные устройства релейной защиты (МУРЗ) без которых невозможно функционирование энергосистемы. При массовых отказах МУРЗ в результате воздействия ЭМИ ЯВ будет крайне затруднительно заниматься настройкой множества комплектов ЗИП МУРЗ одновременно на многих удаленных энергообъектах. Поэтому, комплекты ЗИП МУРЗ, определенных как КВУ, должны не только храниться рядом с действующими МУРЗ, но и должны быть заранее запрограммированы, настроены и конфи-

гурированы для быстрой замены отказавших блоков конкретного МУРЗ, работающего с конкретными настройками и уставками.

Второй вопрос, требующий решения: как хранить ЗИП КВУ? Проблема заключается в том, что ЭМИ ЯВ создает у поверхности земли напряженность электрического поля, доходящую до 50 кВ/м. При такой напряженности поля на выводах даже относительно небольших по размерам электронных компонентов (в пределах одной печатной платы) может возникать разность потенциалов, достаточная для электрического пробоя p-n переходов, тончайших слоев изоляции в микропроцессорах или стирания информации в ячейках элементов памяти. Поэтому комплекты ЗИП КВУ должны храниться в защищенных от ЭМИ ЯВ контейнерах.

Какими свойствами должны обладать эти контейнеры? Обратимся к стандарту MIL-STD-188-125-1 [7.26], оговаривающему требования по эффективности экранирования критически важных объектов от воздействия ЭМИ ЯВ, табл. 7.1.

Табл. 7.1. Минимальные требования по эффективности экранирования критически важных объектов от воздействия ЭМИ ЯВ (по рис. 1 из MIL-STD-188-125-1 [6.26])

Частота излучения	Ослабление, вносимое экраном, дБ
10 кГц	20
100 кГц	40
1 МГц	60
10 МГЦ	80
1ГГц	80

В то же время, стандарт IEC 61000-2-13 [7.27] приводит данные о спектральной плотности излучения различных видов ПЭДВ, рис. 7.11, из которых видно, что для компонентов E1 и E2 (в стандарте E2 обозначен как «молния», поскольку его параметры близки к параметрам молнии) ЭМИ ЯВ плотность излучения остается максимально высокой на частотах ниже 10 кГц и резко снижается уже на частотах выше 300 МГц. Другие источники ПЭДВ (не ЭМИ ЯВ) создают относительно высокую плотность излучения в диапазоне более высоких частот, вплоть до 10 ГГц. Поэтому, эффективная за-

щита должная обеспечиваться в диапазоне частот от единиц килогерц до 10 ГГц.

Как известно, глубина проникновения электромагнитной волны в металлы определяется скин-эффектом и зависит от частоты: чем выше частота (f), тем на меньшую глубину (Δ) проникает волна, то есть, тем тоньше может быть стенка экрана:

$$\Delta = 503\sqrt{\frac{\rho}{\mu_m f}} ,$$

где: Δ – глубина проникновения волны,
ρ – удельное сопротивление металла,
μ_m - магнитная проницаемость металла,
f – частота излучения

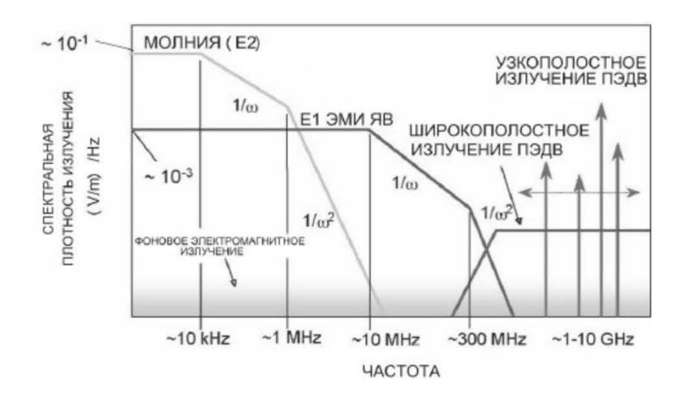


Рис. 7.11. Спектральная плотность излучения различных источников ПЭДВ (из стандарта IEC 61000-2-13)

Глубина проникновения электромагнитной волны – это поверхностный слой металла, в котором напряженность электромагнитного поля снижается в е = 2.718 раза. По данным [7.28] в этом слое будет выделяться почти 86% энергии, поступающей с поверхности. В табл. 7.2 приведены результаты расчета по приведенной выше формуле для наиболее широко используемого в качестве экрана металла – алюминия.

Табл. 7.2. Глубина проникновения электромагнитной волны в стенки экрана из алюминия для различных частот.

Частота	1 кГц	10 кГц	100 кГц	1 МГц	10 МГц	100 МГц	1 ГГц
Глубина проникновения волны, мм	2.6	0.83	0.26	0.083	0.026	0.0083	0.0026

Как можно видеть из таблицы, контейнер из алюминия с толщиной стенки не менее 3 мм может обеспечить достаточно эффективное ослабление излучения всех видов ПЭДВ.

Что же предлагает сегодня рынок защитных контейнеров? Прежде всего, этот рынок широко представлен крупными и тяжелыми толстостенными металлическими контейнерами, рис. 7.12, снабженными защищенными системами вентиляции и фильтрами для вводных кабелей.

Рис. 7.12. Крупные металлические контейнеры-боксы для защиты от ЭМИ ЯВ, снабженные системами вентиляции и фильтрами для подключения внешних кабелей

Такие контейнеры широко применяются в армии и они, безусловно, обеспечивают надлежащую защиту расположенного в них оборудования. К сожалению, это очень дорогие средства защиты,

которые вряд ли можно использовать для хранения ЗИПа в электроэнергетике. Еще одной разновидностью защитного контейнера является комната без окон со стенками и дверями, облицованными медными листами (такие комнаты предлагаются компанией Holland Shielding Systems). Такого рода защитные контейнеры также обладают замечательной экранирующей способностью (от 40 до 120 дБ в частотном диапазоне от 10 кГц до 10 ГГц), но также, как и в предыдущем случае имеют слишком высокую стоимость.

Простыми, надежными и очень дешевыми контейнерами для защиты от ЭМИ ЯВ являются, по заверению их производителей, пластиковые пакеты различных размеров с металлизированным слоем, рис. 7.13.

Рис. 7.13. Пластиковые пакеты с металлизированным слоем, предназначенные для защиты небольших электронных приборов от ЭМИ

Рис. 7.14. Защитный тент (палатка), изготовленный из металлизированной ткани

Как правило, производители таких пакетов указывают высокую степень ослабления излучения, доходящую до 40 – 45 дБ, но при этом скромно умалчивают, для какого частотного диапазона получены эти значения. Может ли металлизированный слой толщиной в несколько микрон эффективно ослаблять электромагнитное поле в частотном диапазоне от килогерц до гигагерц? Таблица 7.2 дает однозначный ответ на этот вопрос: нет, не может!

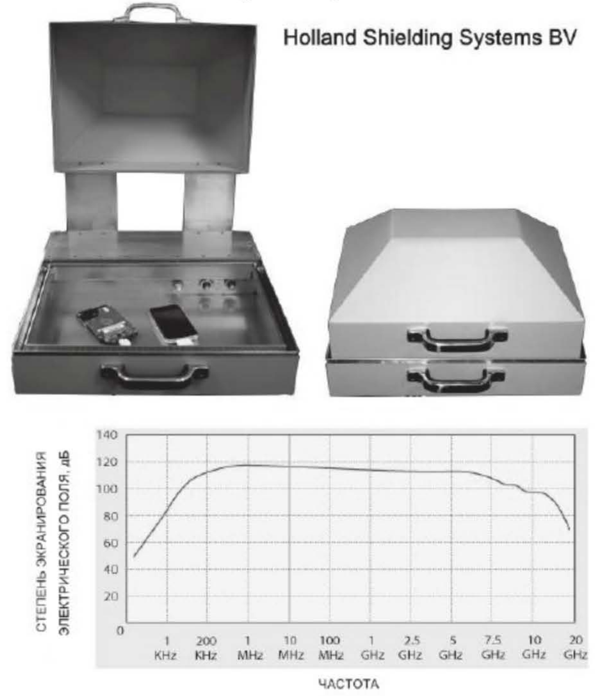


Рис. 7.15. Защитный контейнер компании Holland Shielding Systems BV, обладающий очень высокой экранирующей способностью

Еще одной разновидностью защитного контейнера, также широко представленного на рынке и рекламируемого как надежное средство защиты от ЭМИ ЯВ, является тент (палатка), выполненная из такого же, как и пакеты, металлизированного пластика или, в

лучшем случае, сотканная из ткани, содержащей металлические нити, рис. 7.14.

Специальные переносные толстостенные металлические контейнеры, обеспечивающие очень эффективное экранирование, также широко представлены на рынке, рис. 7.15.

К сожалению, такие контейнеры слишком дороги для хранения ЗИП и имеют недостаточный внутренний объем.

Самыми подходящими, по нашему мнению, являются простые алюминиевые контейнеры, сваренных из листового алюминия в форме простых ящиков с крышками, рис. 7.17. Такие контейнеры с толщиной стенки 3/16 дюйма (4.8 мм) имеют вполне приемлемую степень экранирования: не менее 50 дБ в диапазоне частот 100 кГц – 1 ГГц; (76 дБ при частоте 300 МГц; 66 дБ при частоте 1 ГГц) и выпускаются рядом компаний, в том числе Montie Gear, EMP Engineering и др. по стандартным или индивидуальным размерам.

Рис. 7.17. Недорогие защитные контейнеры для хранения ЗИП, выполненные из листового алюминия

Следует отметить, что такие простые контейнеры нужных размеров могут быть изготовлены в любой мастерской, выполняющей сварочные работы. При этом, с целью предотвращения воздействия электромагнитных полей верхней части частотного диапазона на хранящиеся электронные приборы (которое может проникнуть во внутреннюю полость контейнера через зазоры, образуемые неплотно прилегающей крышкой), рекомендуется особо чувствительные электронные изделия (например, печатные платы с микропроцессорами и элементами памяти) помещать в описанные выше пластиковые металлизированные пакеты перед размещением в контейнерах.

Подводя итоги, можно сделать следующие выводы:

1. Одной из мер быстрого восстановления работоспособности электроэнергетической системы после воздействия того или иного вида ПЭДВ, является создание специальных комплектов ЗИП электронной аппаратуры.
2. Известные методы оптимизации запасов ЗИП неприменимы для рассматриваемого случая.
3. Для обеспечения быстрого восстановления исправности электронной аппаратуры энергосистем должны быть созданы полные комплекты ЗИП для критически важных устройств (КВУ), расположенных на критически важных объектах (КВО) электроэнергетики. КВУ и КВО должны быть заранее определены.
4. Комплекты ЗИП для КВУ должны быть независимы от общих запасов ЗИП, хранящихся на складах.
5. Комплекты ЗИП КВУ должны быть заранее проверены, настроены и конфигурированы и должны храниться в непосредственной близости от КВУ к которым они относятся.
6. Комплекты ЗИП КВУ должны храниться в защищенных от ЭМИ ЯВ и других видов ПЭДВ закрытых контейнерах, которые могут быть изготовлены путем сварки из листов алюминия толщиной около 5 мм. Особо чувствительные блоки, содержащие микропроцессоры и элементы памяти должны быть предварительно помещены в металлизированные пластиковые пакеты.

Литература к Гл. 7

7.1 Коновалова Е. В. Основные результаты эксплуатации устройств РЗА энергосистем Российской Федерации. – Сборник докладов XV научно-технической конференции «Релейная защита и автоматика энергосистем», Москва, 2002.

7.2 Kjolle G.H., Heggset J., Hjartsjo B.T., Engen H. Protection System Faults 1999-2003 and the Influence on the Reliability of Supply // 2005 IEEE St. Petersburg Power Tech, St. Petersburg, Rusia, June 27-30, 2005.

7.3 Гуревич В. И. Проблемы оценки надежности релейной защиты.
"Электричество", 2011, № 2, стр. 28 - 31.

7.4 Гуревич В. И. Испытания микропроцессорных устройств релейной защиты. – Электро: Электротехника. Электроэнергетика. Электротехническая промышленность, 2009, №1, с. 31 – 33.

7.5 A. Bittencourt, M. R. de Carvalho , J. G. Rolim, Adaptive Strategies in Power Systems Protection using Artificial Intelligence Techniques. - The 15th International Conference on Intelligent System Applications to Power Systems, Curitiba, Brazil November 8 - 12, 2009.

7.6 M. A. Laughton, Artificial Intelligence Techniques in Power Systems, In book "Artificial intelligence techniques in power systems", The Institution of Engineering and Technology, 1997, p. 1-18.

7.7 R. Khosla, T. Dillion, Neuro-Expert System Applications in Power Systems. – In book "Artificial intelligence techniques in power systems", The Institution of Engineering and Technology, 1997, 238 – 258.

7.8 Ю.Я. Лямец, Д.В. Кержаев, Г.С. Нудельман, Ю.В. Романов, Многомерная релейная защита – Тезисы докладов Второй Международной научно-технической конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Москва 7–10 сентября 2009 г.

7.9 Т.С. Камель, М.А. Хассан, А. Эль-Моршеди (Cairo University, Египет) Применение систем искусственного интеллекта в дистанционной защите линии электропередачи. – Тезисы докладов Второй Международной научно-технической конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Москва 7–10 сентября 2009 г.

7.10 Булычев А. Нудельман Г. Релейная защита. Совершенствование за счет упреждающих функций - Новости электротехники», № 4(58), 2009.

7.11 Гуревич В. И. Fata Morgana или фантазеры из ВНИИРа. – Электрические сети и системы, 2009, № 6, с. 54 – 57.

7.12 Гуревич В. И. «Интеллектуализация» релейной защиты: благие намерения или дорога в ад? - Электрические сети и системы, 2010, № 5, с. 63 – 67.

7.13 Беляев А.В., Широков В.В., Емельянцев А.Ю. Цифровые терминалы РЗА. Опыт адаптации к российским условиям. – Новости электротехники, 2009, № 5.

7.14 Гуревич В. И. Проблемы стандартизации в релейной защите. – СПб.: Издательство ДЕАН, 2015. - 168 с.

7.15 Гуревич В. И. Актуальные проблемы релейной защиты: альтернативный взгляд. - "Вести в электроэнергетике", 2010, № 3, с. 30 - 43.

7.16 Гуревич В. И. Новая концепция построения микропроцессорных устройств релейной защиты. - "Компоненты и технологии", 2010, № 6, с. 12-15.

7.17 PJM Relay Testing and Maintenance Practices. PJM Interconnection. Relay Subcommittee. Rev. 2/26/04, 2004.

7.18 Жаднов В. Автоматизация проектирования запасов компонентов в комплектах ЗИП: методы и средства. – Компоненты и технологии, 2010, № 5, с. 173 – 176.

7.19 ОСТ 45.66-96 Запасные части, инструменты и принадлежности средств электросвязи. Стандарт отрасли. М.: ЦНТИ «Информсвязь», 1997.

7.20 Зацаринный А. А., Гаранин А. И., Козлов С. В., и др. Особенности расчета комплектов ЗИП в автоматизированных информационных системах в защищенном исполнении. – Системы и средства информатики, 2013, т. 23, № 1, с. 113 – 131.

7.21 Допира Р. В., Лысюк А. П., Цыбенко Д. В., и др. Методика расчета системы обеспечения запасными частями территориально распределенной радиоэлектронной техники. – Программные продукты и системы, 2009, № 1, с. 128 – 130.

7.22 ГОСТ РВ 20.39.303-98. Комплексная система общих требований. Аппаратура, приборы, устройства и оборудование военного назначения. Требования к надежности. Состав и порядок задания. – М.: ИПК Изд-во стандартов, 1998.

7.23 Trimp M. E., Dekker R., Teunter R. H. Optimize initial spare parts inventories: an analysis and improvement of an electronic decision tool. – Report Econometric Institute E1 2004-52, Erasmus University Rotterdam, 2004, 70 p.
7.24 MIL-STD-1388-2. Department of Defense Requirements for a Logistic Support Analysis Record, 1993.
7.25 Love R. E, Stebbins B. F. An Analysis of Spare Parts Forecasting Methods Utilized in the United States marine Corps. – Thesis AD-A184 698, Naval Postgraduate School, Department of the Navy, 1987.
7.26 MIL-STD-188-125-1 High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions; Part 1: Fixed Facilities.
7.27 IEC 61000-2-13: 2005 Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted.
7.28 Промышленные электротермические установки / Н.М. Некрасова, Л.С. Кацевич, И.П. Евтюкова. М.: Госэнергоиздат, 1961. - 415 с.

8. ЗАЩИТА СИЛОВОГО ЭЛЕКТРООБОРУДОВАНИЯ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

8.1. Магнитогидродинамический эффект ЭМИ ЯВ

Магнитогидродинамический эффект ЭМИ (МГД-ЭМИ) является одной из составляющих ЭМИ ЯВ, условно обозначаемой, как компонент Е3.

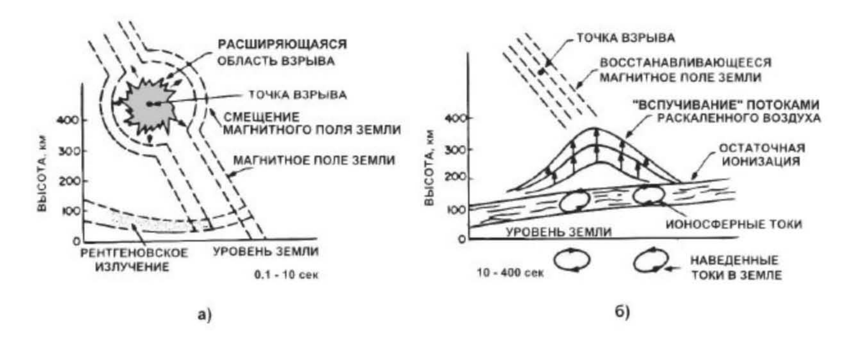


Рис. 8.1. Две стадии магнитогидродинамического эффекта ЭМИ ЯВ [8.1], а) «взрывная волна», б) «вспучивание»

В его основе лежат магнитогидродинамические эффекты взаимодействия плазмы продуктов ядерного взрыва и разогретого ионизированного воздуха с магнитным полем Земли. Различают две стадии этого эффекта, называемые в зарубежной литературе “Blast Wave” («взрывная волна») и “Heave” («вспучивание»), с отличающимися механизмами образования и длительностью, рис. 8.1. Первая стадия с длительностью до 1 - 10 с обусловлена разлетом больших плазменных субстанций, образующихся при взрыве в разреженном воздухе (на большой высоте) и в присутствии магнитного поля Земли. При этом происходит сложное взаимодействие между ионами плазмы, магнитным полем, гамма- и рентгеновским излучениями, сопровождающееся образованием вихревого электрического поля.

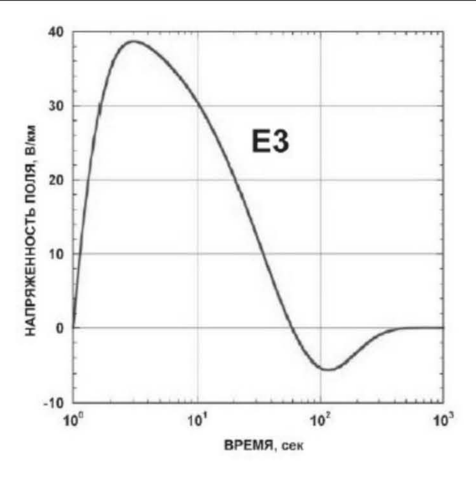


Рис. 8.2. Изменение напряженности горизонтальной составляющей электрического поля на поверхности Земли в результате воздействия компонента Е3 ЭМИ ЯВ [8.2]

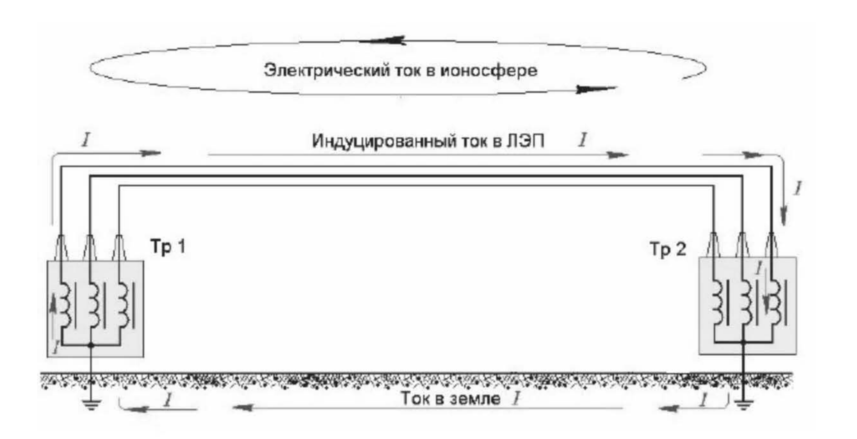


Рис. 8.3. Схема циркуляция токов, наведенных в проводах ЛЭП и замыкающихся через нейтрали силовых трансформаторов

Эти физические эффекты приводят к сильному смещению магнитного поля Земли, которое тем сильнее, чем мощнее энергия взрыва и высота взрыва над поверхностью Земли. На второй стадии происходит вспучивание и быстрый подъем вверх раскаленных в результате взрыва и сильно ионизированных масс воздуха, то есть, фактически, плазмы. Пересечение ионизированной плазмой силовых линий магнитного поля Земли сопровождается поляризации воздушного слоя и генерацией мощного электрического поля, которое, в свою очередь, формирует сильные циркулирующие токи в ионосфере. Процессы эти относительно медленные. Длительность этой фазы взрыва составляет 10 – 300 сек.

Результатом всех этих процессов в разреженной атмосфере является возникновение у поверхности Земли относительно медленно изменяющегося электрического поля с напряженностью в единицы-десятки вольт на километр, рис. 8.2.

Несмотря на небольшую напряженность электрического поля, вызванного компонентом Е3 ЭМИ ЯВ, оно наводит в протяженных металлических предметах (трубах, рельсах, проводах ЛЭП) довольно сильные электрические токи очень низкой частоты (менее 1 Гц), то есть, квазипостоянные токи. Особенно опасными являются токи, наведенные в проводах ЛЭП, рис. 8.3.

8.2. Влияние компонента Е3 ЭМИ ЯВ на силовое электрооборудование

Поскольку геомагнитный индуцированный ток (ГИТ) имеет очень низкую частоту (менее 1 герца), то его воздействие аналогично воздействию постоянного тока и поэтому в первую очередь его влияние будет проявляться на электрооборудовании, содержащем электромагнитные системы, такие, как силовые трансформаторы. Насыщение сердечника силового трансформатора квазипостоянным током в нейтрали приводит к возрастанию тока намагничивания, сильному искажению кривой тока в обмотках трансформатора, существенному увеличению потерь в трансформаторе и росту температуры обмотки и магнитопровода, рис. 8.4. Опасность такого режима работы трансформатора заключается не только в высокой вероятности выхода из строя самого трансформатора, но также и в негативном влиянии его на всю систему электроснабжения.

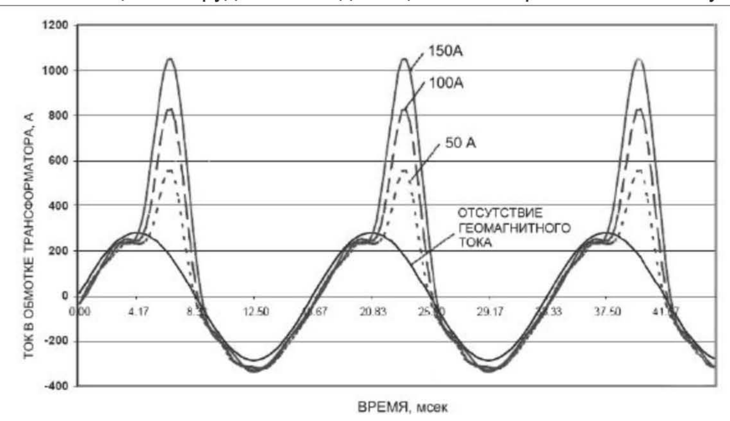


Рис. 8.4. Искажение формы тока в установившемся режиме в обмотках силового трансформатора при протекании в его нейтрали геомагнитных токов величиной 50, 100 и 150А [7.3]

Трансформатор, находящийся в таком режиме является мощным источником четных и нечетных гармоник, вызывающих перегрузку батарей емкостной компенсации и нарушающих нормальную работу релейной защиты. Устройства защиты конденсаторных батарей отключат их, спасая от перегрузки. В сочетании с одновременным резким возрастанием потребления реактивной мощности самим трансформатором, находящимся в таком режиме, и при большой его мощности, это приведет к существенному дефициту реактивной мощности в системе. При этом снижается напряжение и в работу автоматически вступают регуляторы напряжения под нагрузкой самих трансформаторов, пытающиеся восстановить уровень напряжения. Контакторы устройств РПН трансформаторов не предназначены для коммутации токов, содержащих значительную постоянную составляющую и с большой вероятностью будут разрушены, что может привести к повреждению устройства РПН и к короткому замыканию регулировочной части обмоток трансформаторов. В таком режиме должны мгновенно сработать выключатели и отключить поврежденные трансформаторы. Но вот вопрос, способны ли будут высоковольтные выключатели отключить такие токи короткого замыкания и способны ли вообще будут отключать токи нагрузки, содержащие большую постоянную составляющую?

Ведь они не предназначены для коммутации таких токов. А что произойдет с конденсаторами, шунтирующими последовательно соединенные полюса таких выключателей, при воздействии на них высокочастотных гармоник? Вопросов пока больше, чем ответов. Тем не менее, известно, что сильные солнечные бури, вызывающие эффекты, сходные по своим параметрам с эффектами, вызываемыми компонентном Е3 ЭМИ ЯВ, неоднократно приводили к серьезным повреждениям силового электрооборудования и к коллапсу энергосистем в различных странах.

8.3. Защита силового электрооборудования от воздействия геомагнитных индуцированных токов

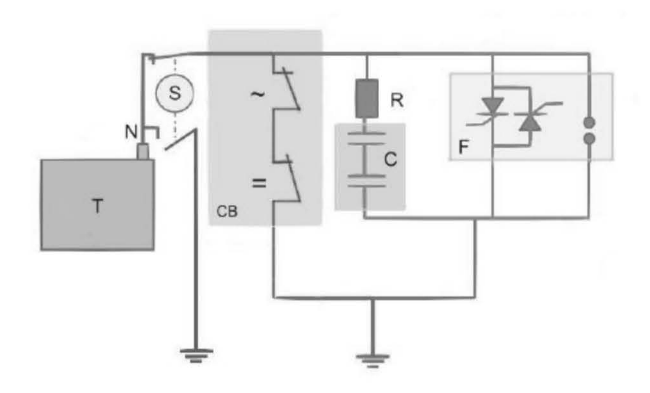
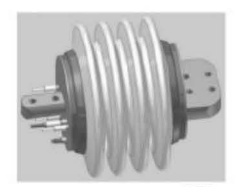


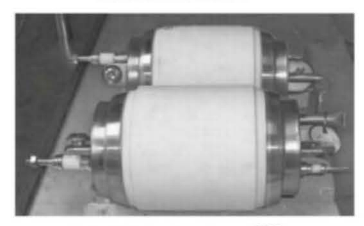
Рис. 8.5. Типовая схема устройства, блокирующего ГИТ в нейтрали силового трансформатора. T – трансформатор, S – коммутационный аппарат, предназначенный для вывода устройства из эксплуатации, CB – специальный выключатель, предназначенный для отключения переменного и постоянного токов, C – батарея конденсаторов, R – ограничительный резистор, F – специальное устройство для защиты от перенапряжений при протекании аварийных токов в цепи нейтрали

Совершенно очевидно, что эффективно защитить установленное силовое электрооборудование энергосистем можно предотвратив протекание через него ГИТ. Этого можно достигнуть либо

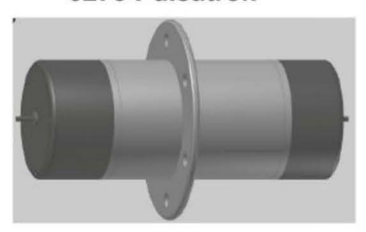
предотвратив протекание ГИТ через провода ЛЭП (при использовании батареи продольной емкостной компенсации, включенных в разрыв проводов ЛЭП), либо блокировав попадание ГИТ в нейтрали силовых трансформаторов (при включении конденсаторов последовательно в цепь заземления нейтрали).



4275 Bi-tron™



3275 Pulsatron™



4138 Bi-tron™

Рис. 8.6. Мощные высоковольтные управляемые разрядники компании Advanced Fusion Systems, типов 4275 (35 кВ, 100 кА); 3275 (500 кВ, 250 кА); 4138 (75 кВ, 250 кА)

Продольная емкостная компенсация – дорогое удовольствие и применяется редко лишь на очень протяженных ЛЭП для компен-

сации индуктивного сопротивления проводов. Поэтому, в последнее время интенсивно разрабатываются установки на основе конденсаторов, предотвращающие попадание ГИТ в нейтрали силовых трансформаторов.

Проблема заключается в том, что в отсутствии ГИТ эти установки не должны влиять на нормальные режимы работы трансформаторов и электрической сети, то есть не должны снижать эффективность заземления нейтрали, должны выдерживать протекание больших токов короткого замыкания и при этом приводить к возникновению феррорезонансных явлений и перенапряжений в переходных режимах. С целью обеспечения этих условий, во всех типах установок такого рода принят такой алгоритм работы, при котором батарея конденсаторов постоянно зашунтирована байпасным силовым коммутационным элементом (СВ) и вводится в работу путем дешунтирования (размыкания этого коммутационного элемента) лишь в момент обнаружения ГИТ, рис. 8.5.

Возникновение аварийных режимов в сети с включенными в нейтраль конденсаторами может привести к появлению очень высоких напряжений в цепи нейтрали трансформатора, превышающих уровень изоляции нейтрали, а также и на самих конденсаторах. Поэтому, такие установки должны быть снабжены специальными устройствами защиты от перенапряжений F (обычные варисторы для этого непригодны). Ни рис. 8.5 условно показано защитное устройство, содержащее блок из 6 мощных высоковольтных тиристоров и вакуумный разрядник. На практике вместо блока тиристоров широко применяют также и мощные управляемые трехэлектродные разрядники специальной конструкции, рис. 8.6.

Кроме того, должна быть предусмотрена возможность отключения этой установки специальным коммутационным аппаратом (S) типа отделителя с заземляющим ножом для вывода устройства из эксплуатации без отключения трансформатора. В целом, установка получается совсем не простой и не дешевой (более 300 тыс. долларов США), рис. 8.7.

Существуют и другие методы защиты силовых трансформаторов от ГИТ, основанные на изменении конструкции трансформатора. Введение дополнительных немагнитных зазоров в магнитопровод трансформатора снижает вероятность его насыщения, однако ухудшает основные технические характеристики трансформатора.

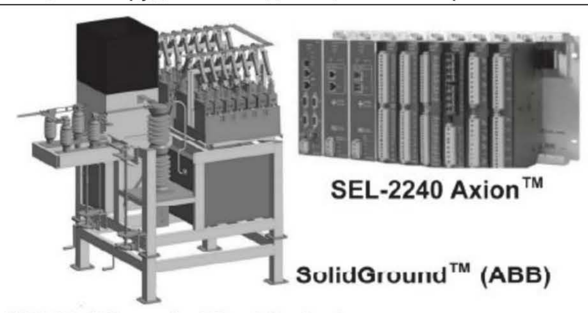


Рис. 8.7. Установки для блокирования ГИТ в цепях нейтрали силовых трансформаторов. Вверху установка, предлагаемая компанией АББ, снабженная контроллером фирмы SEL, внизу установка, разработанная компанией Phoenix Electric

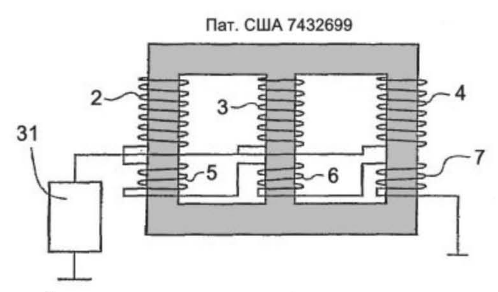


Рис. 8.8. Устройство силового трансформатора с дополнительной обмоткой, компенсирующей ГИТ, 2-4 – основные обмотки; 5-7 – компенсационные обмотки; 31 – элемент с высоким сопротивление к постоянному току и низким сопротивлением к переменному току

Другие известные технические решения, рис. 8.8, предусматривают размещение на магнитопроводе трансформатора дополнительных обмоток, компенсирующих влияние постоянного тока, зашунтированных неким специальным элементом (31), имеющим высокое сопротивление для постоянного тока и низкое сопротивление для переменного тока.

По-видимому, таким элементом может служить батарея конденсаторов, хотя об этом напрямую в патенте США № 7432699 и не упоминается. Аналогичное техническое решение описано и в патенте США № 7489485. В других технических решениях предлагается подключить эту компенсационную обмотку к внешнему регулируемому источнику постоянного тока, компенсирующего ГИТ. Имеются предложения соединять обмотки трансформатора по схеме «обратного зигзага», при которой происходит взаимная компенсация намагничивающих токов каждой фазы, имеющих одинаковую величину, но противоположное направление, и насыщения магнитопровода не происходит.

Все эти технические решения требуют изменения технологии изготовления силовых трансформаторов, ухудшают их технические характеристики и ведут к их существенному удорожанию. То есть, любые технические мероприятия, направленные на предотвращение/компенсацию токов ГИТ, связаны со значительными материальными затратами. В связи с чем, возникает вопрос об экономической целесообразности вложения значительных средств с целью предотвращения повреждения электрооборудования во время такого исключительного события, как высотный ядерный взрыв.

Ряд ведущих мировых производителей мощных высоковольтных трансформаторов (Siemens, ABB и др.) сообщает о разработке ими специальных трансформаторов (GIC Safe Power Transformers), способных выдержать в течение нескольких часов ГИТ величиной до 50 А, а в течение нескольких часов и отдельные импульсы ГИТ с амплитудой до 200 А. В своих рекламных материалах производители не раскрывают технические решения, благодаря которым им удалось повысить устойчивость трансформаторов к ГИТ, но очевидно, что речь не идет о каких-то технических решениях, блокирующих попадание квазипостоянного тока в нейтраль трансформатора или компенсирующих магнитные потоки в магнитопроводе, поскольку при использовании таких технических решений не суще-

ствует ограничений по времени воздействия ГИТ и нет таких жестких ограничений по его величине.

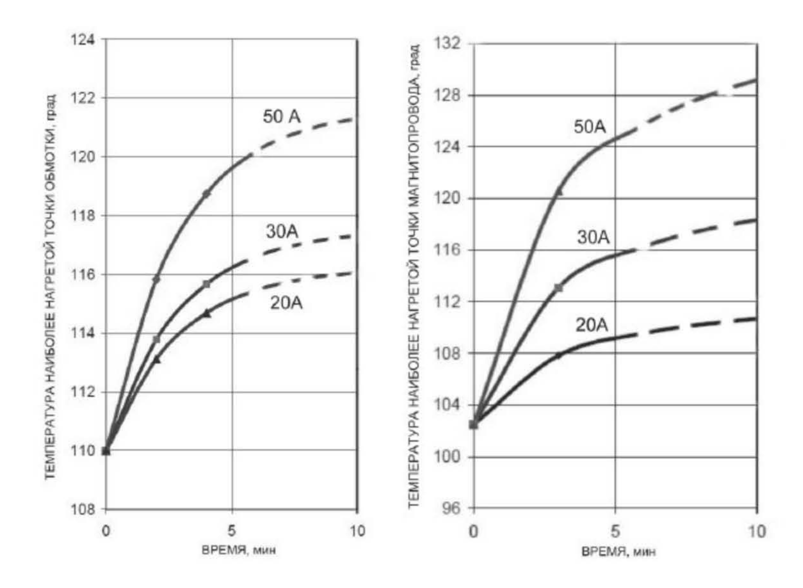


Рис. 8.9. Примеры графиков нагрева обмотки и магнитопровода силового трансформатора при протекании в его нейтрали геомагнитных токов величиной 20, 30 и 50А

Скорее всего, такие трансформаторы просто более устойчивы к повышенной температуре за счет использования специальных высокотемпературных лаков для изоляции пластин магнитопровода и специальных изоляционных материалов для обмоток.

Повышение устойчивости трансформатора к квазипостоянным токам, протекающим через него, вовсе не является полноценным решением проблемы, поскольку, как было показано выше, трансформатор с насыщенным магнитопроводом является источником серьезных проблем для многих других видов силового электрооборудования, поэтому сохранение работоспособности трансформатора отнюдь не гарантирует работоспособности системы электроснабжения.

Вряд ли можно признать целесообразным вложение значительных денежных средств для защиты энергосистем от одиночного события, вероятность возникновения которого достаточно низка. Так в чем же здесь дело и почему такого рода защитные устройства разрабатываются и предлагаются на рынке? Дело в том, что ГИТ возникает не только во время высотного ядерного взрыва, но и во время сильных солнечных бурь, которые повторяются периодически и являются причиной тяжелых аварий в энергосистемах. Однако, влияние солнечных бурь на различные регионы Земли не одинаковы. Это влияние усиливается по мере приближения к полюсам Земли и очень слабо в районах, прилегающих к экватору. В регионах, значительно удаленных от полюсов, солнечные бури не вызывают сколько-нибудь заметных ГИТ, способных повлиять на работоспособность энергосистем. Однако, разработчики защитных устройств обычно указывают на то обстоятельство, что параметры ГИТ, возникающего от солнечных бурь и от высотного ядерного взрыва, во многом схожи между собой и поэтому энергосистемы, желающие повысить устойчивость электрооборудования к высотному ядерному взрыву, должны применять такие защитные устройства независимо от их географического расположения. Казалось бы, все вполне логично.

Однако, существует одно важное отличие в параметрах ГИТ, возникшего как результат мощной вспышки на солнце и в результате высотного ядерного взрыва, ставящее под сомнение обоснованность такой логики. Это отличие – длительность существования ГИТ. При высотном ядерном взрыве длительность существования ГИТ составляет лишь несколько минут, в течение которых силовые трансформаторы, обладающие большой теплоемкостью, просто не успеют нагреться до опасной температуры, рис.8.9.

Понятно, что при больших значениях ГИТ, температура частей трансформатора будет более высокой, но за столь короткое время она, все же, не достигнет опасных для трансформатора значений. Значительно большую опасность представляют собой токи, искаженные несимметрично насыщенным трансформатором, для других видов силовой аппаратуры, рассмотренных выше, которые не обладают такой инерцией, как силовые трансформаторы. Однако, если во время солнечной бури ГИТ присутствуют на протяжении многих часов, в течение которых должно сохраняться электроснабжение

потребителей, то при высотном ядерном взрыве время существования ГИТ ограничивается несколькими минутами, в течение которых электрооборудование может быть выведено из работы во избежание его повреждения, а затем снова возвращено в работу. При этом, поскольку процесс нарастания ГИТ достаточно медленный, можно отключить трансформаторы сразу же при обнаружении постоянной составляющей в токе нейтрали, не дожидаясь насыщения его магнитопровода и всех последующих за этим событий. Такой метод защиты силового электрооборудования энергосистем от магнитогидродинамического эффекта ЭМИ ЯВ нам представляется значительно более правильным, чем рассмотренные выше, поскольку обладая высокой эффективностью, он не требует значительных материальных затрат. Все затраты на реализацию такого метода защиты сводятся к установке специального реле, реагирующего на появление постоянной составляющей в токе нейтрали и мгновенно выдающего команду на отключение трансформатора.

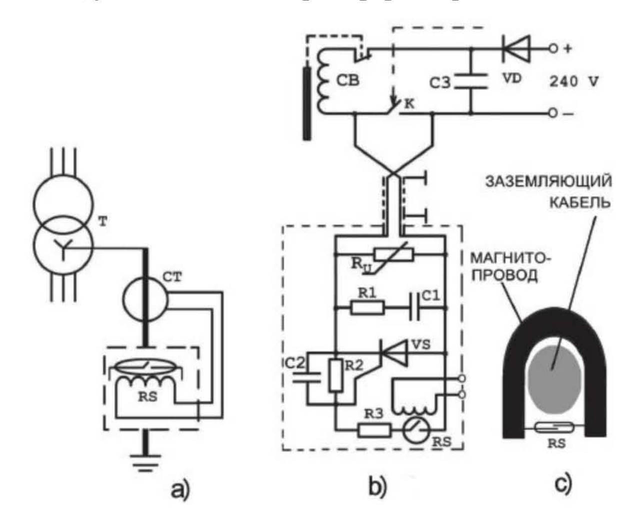


Рис. 8.10. Реле защиты силового трансформатора от низкочастотного индуцированного геомагнитного тока в цепи нейтрали

Такое реле должно иметь специальную конструкцию, а не такую, какую компания АББ использовала для управления устрой-

ством SolidGround (промышленный программируемый контроллер типа SEL-2240), поскольку речь идет об устройстве защиты от составляющей E3 ЭМИ ЯВ, появляющейся вслед за составляющими E1 и E2, которые с большой вероятностью выведут из строя микропроцессорное управляющее устройство SEL-2240 еще до того, как оно успеет сработать.

На рис. 8.10а показан принцип действия реле, чувствительного к постоянной составляющей тока в нейтрали силового трансформатора и нечувствительного к переменному току, изменяющемуся в широких пределах. Реле состоит из геркона RS с обмоткой, размещенного на кабеле, соединяющем нейтраль трансформатора с точкой заземления, перпендикулярно к оси кабеля и тороидального трансформатора тока CT, установленного на этом кабеле. При отсутствии постоянной составляющей в токе нейтрали, магнитное поле кабеля, воздействующее непосредственно на геркон, полностью компенсируется магнитным полем катушки, одетой на геркон, питающейся от трансформатора тока. Изменение переменного тока, протекающего в нейтрали, приводит к пропорциональному изменению обоих магнитных полей, воздействующих на геркон, и к их взаимной компенсации. В случае появления значительной постоянной составляющей в токе нейтрали (более 10 - 15 А) баланс магнитных полей, воздействующих на геркон, нарушается: магнитное поле кабеля по-прежнему воздействует на него, а компенсирующее магнитное поле катушки, запитанной от трансформатора тока, нет, поскольку постоянная составляющая тока не трансформируется через трансформатор тока. В результате, геркон срабатывает. Реальная схема реле включает дополнительно усилитель мощности на тиристоре VS, варистор R_U и цепочку R1C1, защищающие тиристор от помех и перенапряжений, рис. 10в. Реле снабжено сплошным электростатическим экраном и ферромагнитным экраном, имеющим окно лишь со стороны кабеля в месте расположения геркона и соединено с цепью отключающей катушки выключателя CB посредством специального экранированного кабеля с витыми парами и многослойным комбинированным экраном, заземленным с двух концов, устойчивым к воздействию электромагнитного импульса. В реле могут использоваться миниатюрные высоковольтные вакуумные герконы, например, типа KSK-1A85 (производства компании Meder Electronics), с электрической прочностью изоляции между

контактами 4000 В при диаметре колбы 2.75 мм и длине 21 мм. Этот геркон способен коммутировать нагрузку мощностью до 100 Вт (максимальное коммутируемое напряжение 1000 В; максимальный коммутируемый ток 1А); время срабатывания 1 мс; максимальная чувствительность 20А. При необходимости увеличения чувствительности могут быть использованы дополнительные ферромагнитные элементы (концентраторы магнитного поля), расположенные в области геркона, рис. 10с. Для получения реле с более низкой чувствительностью и более высоким порогом срабатывания, продольная ось геркона должна образовывать угол, отличный от 90º с осью кабеля, на котором он установлен. Тиристор тоже выбран миниатюрным высоковольтным, типа SKT50/18E (производства компании Semicron), с максимальным напряжением 1800В и максимальным длительным током 75А, выдерживающий высокие скорости нарастания напряжения (1000В/мкс) и широкий диапазон рабочих температур (-40+130ºС). Цепь питания отключающей катушки снабжена накопительным конденсатором С3, обеспечивающим срабатывание выключателя даже при пропадании оперативного напряжения. Цепочка R2C2 предназначена для дополнительного повышения помехоустойчивости устройства. Конденсатор С2 обеспечивает некоторую задержку включения тиристора, предотвращая его отпирание под действием мощной импульсной помехи.

Применение в реле дискретных высоковольтных компонентов вместо традиционной микроэлектроники позволяет обеспечить его высокую надежность в условиях воздействия ЭМИ ЯВ.

На основании вышеизложенного, можно сделать следующие выводы:

1. Магнитогидродинамический эффект ЭМИ ЯВ (МГД-ЭМИ), заключающийся в появлении квазипостоянного тока, протекающего через нейтрали силовых трансформаторов, отрицательно влияет не только на сами трансформаторы, но и на многие другие виды силового электрооборудования, в первую очередь на батареи конденсаторов и высоковольтные выключатели. Поэтому, технические решения, направленные на защиту от влияния МГД-ЭМИ должны предусматривать защиту не только самих трансформаторов, но и всех других видов силового электрооборудования энергоси-

стем. Технические решения, направленные не на блокирование или компенсацию геомагнитных индуцированных токов (ГИТ), а лишь повышающих устойчивость трансформаторов к протеканию через них таких токов, нельзя признать эффективными.

2. Существующие технические решения, основанные на предотвращении насыщения магнитопроводов трансформатора можно условно разделить на две группы:
   - использование внешних установок, включаемых в разрыв нейтрали трансформатора и блокирующих протекание квазипостоянного тока в цепи нейтрали;
   - внутренние конструктивные изменения самого трансформатора (его обмоток или магнитопровода), препятствующих насыщению магнитопровода при протекании квазипостоянного тока в цепи нейтрали.

   Любые из известных технических решений, направленных на сохранение нормального функционирования энергосистемы во время воздействия на ее элементы ГИТ связаны со значительными материальными затратами.
3. Несмотря на схожесть большинства параметров ГИТ, возникающих в результате высотного ядерного взрыва (составляющая Е3) и в результате сильных солнечных бурь, между ними имеется одно существенное отличие: длительность существования ГИТ. Это отличие диктует необходимость различных подходов к защите электрооборудования от воздействия солнечных бурь и составляющей Е3 ЭМИ ЯВ.
4. Использование известных технических решений по защите силового электрооборудования энергосистем от воздействия составляющей Е3 ЭМИ ЯВ нельзя признать экономически обоснованным. Для этого случая является оправданным кратковременное отключение силового трансформатора на несколько минут по сигналу специального реле, с последующим автоматическим возвратом его в работу.
5. Реле, выдающее команду на отключение трансформатора, должно иметь специальную конструкцию, обеспечивающую его работоспособность при воздействии всех компонентов ЭМИ ЯВ.

Литература к Гл. 8

8.1 Study to Access the Effects of Magnetohydrodinamic Electromagnetic Pulse on Electric Power Systems. – Report ORNL/sub-83/43374/1/v, Oak Ridge National Laboratory, 1985.

8.2 IEC 61000-2-9 Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance, 1996.

8.3 The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid. – Report Meta-R-321, Metatech Corp., 2010.

СОДЕРЖАНИЕ

КНИГИ ПОЧТОЙ

Заказ можно оформить
на сайте издательства
www.infra-e.ru

№ п/п	Наименование книги	Кол-во
1	**Надежность цифровых устройств релейной защиты.** Показатели. Требования. Оценки	
2	**Устройства электропитания релейной защиты.** Проблемы и решения	
3	**Уязвимости микропроцессорных реле защиты.** Проблемы и решения	
4	**Микропроцессорные реле защиты.** Устройство, проблемы, перспективы	
5	**Внутренние электромонтажные работы**	
6	**Справочник цехового энергетика**	
7	**Справочник инженера по наладке, совершенствованию технологии и эксплуатации электрических станций и сетей.** Централизованное и автономное электроснабжение объектов, цехов, промыслов, предприятий и промышленных комплексов.	
8	**Конструирование источников питания усилителей мощности звуковой частоты**	

ГУРЕВИЧ Владимир Игоревич

ЗАЩИТА ОБОРУДОВАНИЯ ПОДСТАНЦИЙ ОТ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА

Учебно-практическое пособие

Редактор
О.М. Зеленина

Верстка
И.А. Моисеев

Подписано в печать 27.09.2015
Формат 60x84/16. Бумага офсетная.
Гарнитура «Таймс».
Тираж 300 экз. Заказ №221

Издательство «Инфра-Инженерия»
Тел.: 8(911)512-48-48
E-mail: infra-e@yandex.ru
www.infra-e.ru